Ruckus Wireless™ ZoneFlex™ Outdoor Access Point

Release 9.8.1 User Guide

For the following ZoneFlex and SmartCell outdoor Access Points:
- ZoneFlex 7761-CM Dual-Band 802.11n AP with Integrated Cable Modem
- ZoneFlex 7762, 7762-AC, 7762-S, 7762-S-AC and 7762-T Dual-Band 802.11n APs
- ZoneFlex 7781CM Dual-Band 802.11n AP with Integrated Cable Modem
- ZoneFlex 7782, 7782-E, 7782-N and 7782-S Dual-Band 802.11n APs
- SmartCell 8800-S Outdoor Access Point
- T300 Omni 802.11ac Outdoor Access Point
- T301n 30-Degree Narrow Sector 802.11ac Outdoor Access Point
- T301s 120-Degree Wide Sector 802.11ac Outdoor Access Point

Part Number 800-70598-001 Rev B
Published July 2014

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Copyright 2014. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, ChannelFly, SmartCell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide

Related Documentation 6
Document Conventions 8
Documentation Feedback 9

1 Introducing the ZoneFlex Access Point

Overview of the ZoneFlex Access Point 11
Installing the Access Point 12
Getting to Know the Access Point Features 13
ZoneFlex 7761-CM Cable Modem Access Point 14
CMAP Connectors 16
CMAP Ethernet/PoE-Out Port 17
CMAP LEDs 17
CMAP Supported Power Sources 18
CMAP Heaters 18
CMAP Operation 18
ZoneFlex 7762 Access Point 19
ZoneFlex 7762-AC Access Point 22
ZoneFlex 7762-S Access Point 25
7762-S 5GHz Antenna Connectors 27
ZoneFlex 7762-S-AC Access Point 28
ZoneFlex 7762-T Access Point 31
ZoneFlex 7781CM Access Point with Cable Modem 34
Reading the 7781CM LEDs 37
LED Boot Sequence 37
LED Online/Steady State 37
Reading LEDs in Access Point Mode 38
Reading LEDs in Cable Modem Mode 39
Powering Options 39
Cable Modem Heater 40
7781CM Operation 40
ZoneFlex 7782 Access Point 41
ZoneFlex 7782-E Access Point 43

ZoneFlex 7782-N Access Point 46
ZoneFlex 7782-S Access Point 48
SmartCell SC8800-S Outdoor Access Point 50
T300 Outdoor Access Point 55
T301n Outdoor Access Point 58
T301s Outdoor Access Point 61

2 Navigating the Web Interface

Logging Into the ZoneFlex AP Web Interface 64
Navigating the Web Interface 65
When Using a Dual-Band Access Point 66

3 Configuring the Access Point

Configuring Device Settings 68
Configuring Internet Settings 70
VLAN Settings Overview 70
Configuring an NTP Server 71
Configuring the Management VLAN 71
Default IP Addressing Behavior 71
Obtaining and Assigning an IP Address 72
DHCP/Auto Configuration 72
Configuring a Static IP 74
PPPoE 75
Configuring L2TP Connection Settings 76
Configuring Local Subnets 78
Configuring Wireless Settings 80
Configuring Common Wireless Settings 80
Reviewing Common Advanced Settings 83
Configuring Wireless # Settings 85
Using WEP 88
Using WPA 90
Customizing 802.1X Settings 93
Setting Threshold Options 95
Rate Limiting 97
Controlling Access to the Wireless Network 97
Configuring Ethernet Ports 100
Setting Ethernet Port Type 103
Trunk Port 103
Access Port 103

General Port 104
Working with Port-Based VLANs 104
Working with 802.1X on Wired Ethernet Ports 104
Configuring Hotspot Service 106
Customizing Hotspot Optional Settings 107
Creating a Hotspot Walled Garden 110
Removing Entries from the Walled Garden Hosts Table 111
Allowing Unrestricted Hotspot Access by MAC Address 111

4 Managing the Access Point

Viewing Current Device Settings 114
Viewing Current Internet Connection Settings 115
Viewing Current Local Subnet Settings 116
Viewing Current Wireless Settings 117
Viewing Associated Wireless Clients 119
Changing the Administrative Login Settings 120
Enabling Other Management Access Options 121
Viewing FlexMaster Management Status 124
Pointing the AP to FlexMaster 125
Working with Event Logs and Syslog Servers 126
Enabling Logging and Sending Event Logs to a Syslog Server 126
Sending a Copy of the Log File to Ruckus Wireless Support 127
Saving a Copy of the Log File to Your Computer 127
Saving a Copy of a Support File to Your Computer 128
Upgrading the Firmware 129
Upgrading Manually via FTP or TFTP 129
Upgrading Manually via the Web 130
Upgrading Manually via Local File 130
Scheduling Automatic Upgrades 130
Rebooting the AP and Cable Modem 132
Resetting the AP to Factory Defaults 133
Running Diagnostics 134
Where to Find More Information 136

Index

About This Guide

This guide describes how to configure and manage the Release 9.8.1 Ruckus Wireless ZoneFlex Access Point. This guide is written for those responsible for managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE This guide assumes that the ZoneFlex Outdoor APs have already been installed as described in the corresponding Installation Guide or Getting Started Guide. Refer to the Installation Guide or Getting Started Guide that shipped with your product for model-specific installation instructions.

NOTE If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at

https://support.ruckuswireless.com/documents.

Related Documentation

In addition to this *User Guide*, each ZoneFlex Access Point documentation set includes the following:

- *Installation Guide/Getting Started Guide/Mounting Guide (for some APs):* Provides essential installation and configuration information to help you get the AP up and running within minutes.
- *Online Help:* Provides instructions for performing tasks using the Access Point's Web interface. The online help is accessible from within the Web interface.
- *Release Notes:* Provide information about the current software release, including new features, enhancements, and known issues.

NOTE If you plan to manage your ZoneFlex Access Points using ZoneDirector, then refer to the *ZoneDirector User Guide* (available from the Ruckus Wireless website).

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs.**
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- ZoneFlex Outdoor Access Point 9.8.1 User Guide
- Part number: 800-70598-001 Revision B
- Page 11

Please note that we can only respond to comments and questions about Ruckus Wireless product documentation at this email address. Questions related to technical support or sales should be directed in the first instance to your network supplier.

Introducing the ZoneFlex Access Point

1

In this chapter:

- Overview of the ZoneFlex Access Point
- Installing the Access Point
- Getting to Know the Access Point Features

Overview of the ZoneFlex Access Point

Congratulations on your purchase of the Ruckus Wireless ZoneFlex Access Point! ZoneFlex Access Points are the industry's most easy to use, yet robust and feature-rich Wi-Fi Access Points designed to bring power and simplicity together for large-scale outdoor deployments.

Your ZoneFlex Access Point uses BeamFlex, a patented antenna technology from Ruckus Wireless that allows wireless signals to navigate around interference, extend wireless signal range, and increase speeds and capacity for wireless networks. The BeamFlex antenna system consists of an array of high-gain directional antenna elements that allow ZoneFlex Access Points to find quality signal paths in a changing environment, and sustain the baseline performance required for supporting data, audio and video applications.

In addition to Ruckus Wireless' proprietary BeamFlex technology, ZoneFlex 7782 Access Point models also support chip level transmit beamforming (TxBF), which complements BeamFlex to provide enhanced interference mitigation.

Your ZoneFlex Access Point can be deployed in standalone mode or as part of the ZoneFlex Smart WLAN system, in which it can be managed by either FlexMaster or ZoneDirector WLAN controller.

NOTE For more information on the ZoneFlex system (including FlexMaster and ZoneDirector), BeamFlex, transmit beamforming, and other Ruckus Wireless technologies, visit www.ruckuswireless.com.

Installing the Access Point

This User Guide assumes that the ZoneFlex Outdoor APs have already been installed and have already been initially configured as described in the corresponding *Installation Guide* or *Getting Started Guide*.

NOTE DO NOT connect the Access Point to your live network when first connecting the AP to an administrative computer. If you connect it to a live network with an active DHCP server, then the AP will acquire a new IP address from DHCP and you will be unable to access it via the default IP address (192.168.0.1).

If the AP has a new IP address, then reset the AP to the factory configuration as described in the corresponding installation guide.

Because of different mounting and wiring procedures, each outdoor AP model has its own installation guide. Refer to the installation guide that shipped with your product for model-specific installation instructions. These documents are available from

support.ruckuswireless.com.

Getting to Know the Access Point Features

This section identifies the physical features of each ZoneFlex Access Point model that is discussed in this guide. Ruckus Wireless recommends that you become familiar with these features.

- ZoneFlex 7761-CM Cable Modem Access Point
- ZoneFlex 7762 Access Point
- ZoneFlex 7762-AC Access Point
- ZoneFlex 7762-S Access Point
- ZoneFlex 7762-S-AC Access Point
- ZoneFlex 7762-T Access Point
- ZoneFlex 7781CM Access Point with Cable Modem
- ZoneFlex 7782 Access Point
- ZoneFlex 7782-E Access Point
- ZoneFlex 7782-N Access Point
- ZoneFlex 7782-S Access Point
- SmartCell SC8800-S Outdoor Access Point
- T300 Outdoor Access Point
- T301n Outdoor Access Point
- T301s Outdoor Access Point

NOTE This guide does not include information on ZoneFlex Indoor Access Points, ZoneFlex 7731 Wireless Bridge, or ZoneFlex 7025 or 7055 Multimedia Wi-Fi Wall Switches. For information on those ZoneFlex models (along with Ruckus Wireless MediaFlex and MetroFlex product lines), refer to their respective documents available from support.ruckuswireless.com.

If you want to extend the range of your wireless network, you can connect an external high gain antenna to the standard N-type radio frequency (RF) antenna connector on the top panel of the Access Point. The antenna must have a gain of less than 9dBi to comply with FCC and CE regulations.

ZoneFlex 7761-CM Cable Modem Access Point

NOTE ZoneFlex 7761-CM requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 1 and Figure 2 identify the 7761-CM Cable Modem AP (CMAP) external features.

Figure 1. CMAP parts and connectors (Connector side)

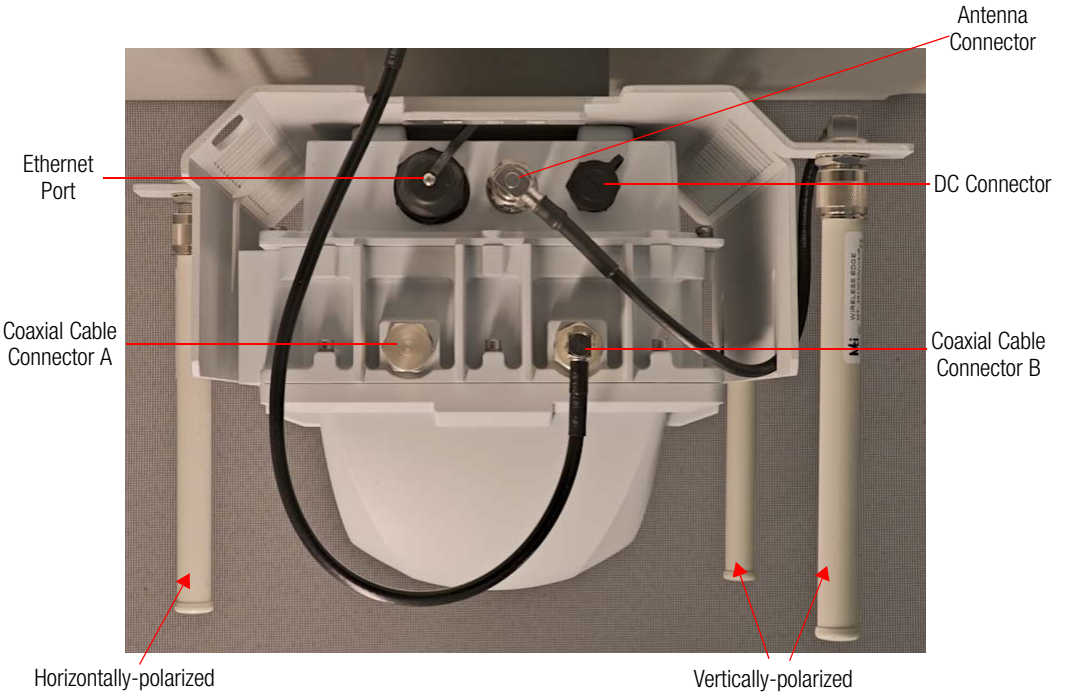


Table 3. Connector-side parts and connectors on the CMAP

Label	Description
Ethernet Port	RJ45 port that supports 10/100Mbps connections and provides Power over Ethernet (PoE) power to compliant devices.
Antenna Connector	One of the three connectors for the three 5GHz antennas supplied with the CMAP. The other two connectors are located on the other side of the unit *(see* Figure 2*)*.
DC Connector	In addition to the power supplied by the coaxial cable from the CMTS, the CMAP may also be DC powered. Shorting pins 3 and 4 in the DC power connector using an electrical shunt resets the CMAP to factory default settings.
Coaxial Cable Connector A	Provides a +/-3dB sample of the downstream RF signal as seen by the cable modem. Refer to the ZoneFlex *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for more information on the CMAP signal levels.
Coaxial Cable Connector B	Connects to the cable modem termination system (CMTS) at the headend using a tap on the plant and it provides AC power to the CMAP. AC power is supplied via Power Over Cable (POC).

Figure 2. CMAP parts and connectors (LED side)

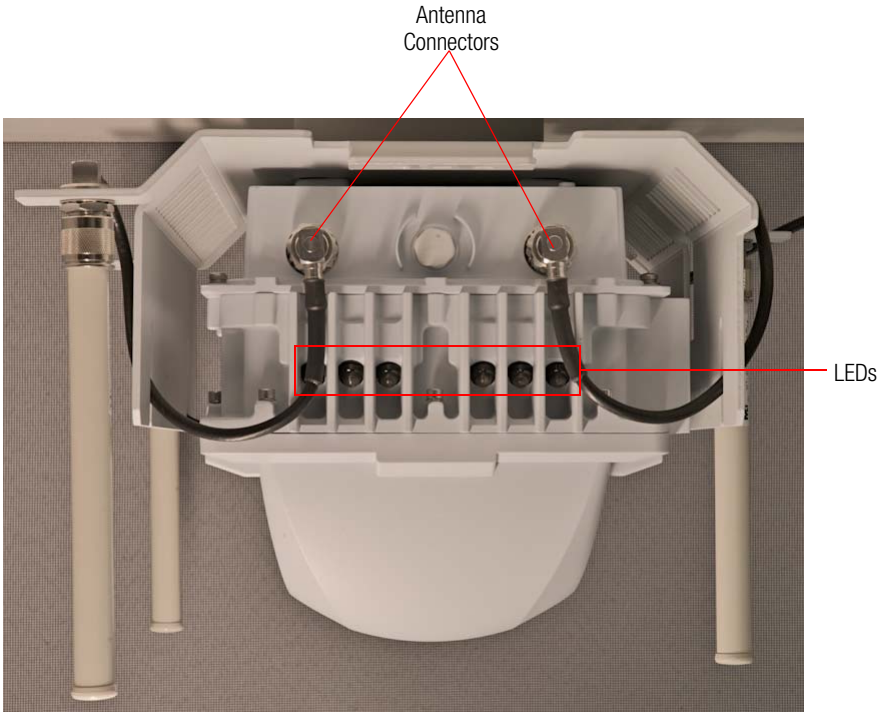


Table 4. LED-side parts and connectors on the CMAP

Label	Description
Antenna Connectors	*Two of the three connectors for the 5GHz antennas. The other connector is located on the other side of the unit (see Figure 1).*
LEDs	Six LEDs that indicate the status of the CMAP and cable modem. For more information, refer to "CMAP LEDs" on page 17.

CMAP Connectors

The CMAP provides the following connectors:

- PoE-Out connector: RJ-45 port that can supply power to devices that support PoE.
- Three N-type antenna connectors: Connects to the three 5GHz antennas (not supplied, with the CMAP).

- DC power supply (Ruckus Wireless part number 705-60244-002): Connected through a 4-pin connector, which is normally unused. It may be used to supply DC power to the unit for testing or configuration. The supply has a reset switch that may be used to reset the unit.
- Coaxial cable connectors (see Figure 1): Connector A may be connected to a spectrum analyzer or signal analyzer to allow monitoring of the downstream signal. Connector B must be connected to the CMTS backbone and AC power when deployed in the field.

CMAP Ethernet/PoE-Out Port

The CMAP provides one 10/100Mbps RJ45 Ethernet port, which also functions as a PoE-Out port. The PoE-Out port, which can supply up to 15.4 watts (compliant with 802.3af), can be used to power PoE-capable devices (for example, a 3G/4G small cell radio or an IP-based surveillance camera).

NOTE The PoE-Out function is non-operational when the unit is powered via the 12 VDC connector.

NOTE By default, both Ethernet data and PoE-Out are enabled. If necessary, you can disable PoE-Out from the Web interface.

CMAP LEDs

Use the six LEDs to check the status of the access point and cable modem. The LEDs behave differently when the access point is in standalone mode and when ZoneDirector is managing it. Upon bootup, the LEDs are in *CM (Cable Modem) Mode*. Once bootup is completed, the LEDs alternate between *CM Mode* and *AP Mode*.

Refer to the ZoneFlex *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for more information on the CMAP LED operation.

NOTE The LEDs also do not indicate whether the AP is in standalone mode or if ZoneDirector is managing the AP. To check if ZoneDirector is managing the access point, log into the ZoneDirector Web interface, go to the *Access Points* page, and then search for the access point's MAC address. If you are unable to find the access point, then it is very likely in standalone mode. If you have multiple ZoneDirector devices on the network, make sure you check each one of them.

CMAP Supported Power Sources

The CMAP supports the following power sources:

- Power over Cable (POC): 40 to 90 VAC supplied through the RF coaxial cable (attached to Connector B) that is connected to the cable modem termination system (CMTS) backbone. POC is the primary and conventional source of power for the CMAP.
- DC power (via DC connector): External 12 VDC. Use this only when staging or debugging the CMAP.

NOTE PoE output is disabled when the CMAP is powered via the 12 VDC connector.

CMAP Heaters

The CMAP includes two built-in heaters (one for the access point and one for the cable modem) that permit operation at extremely low temperatures. They are typically on below 0º C (32º F).

The heaters are enabled by default. If preferred, the access point heater can be disabled from the Web interface. The cable modem heater cannot be disabled.

CMAP Operation

Refer to the *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for information on the Cable Modem configuration and operation procedures.

ZoneFlex 7762 Access Point

NOTE ZoneFlex 7762 requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 3 and Figure 4 identify the Access Point external features.

Figure 3. 7762 Access Point parts

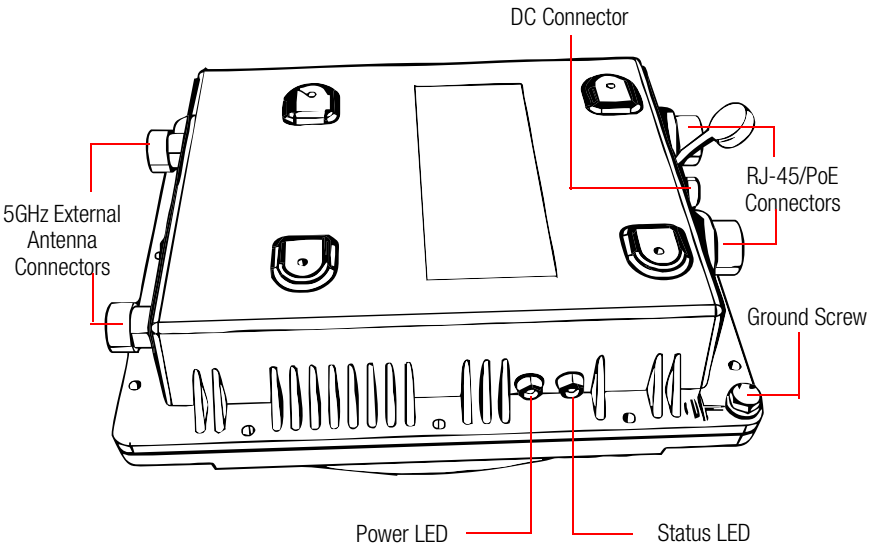


Table 5. LEDs and connectors on the 7762 AP

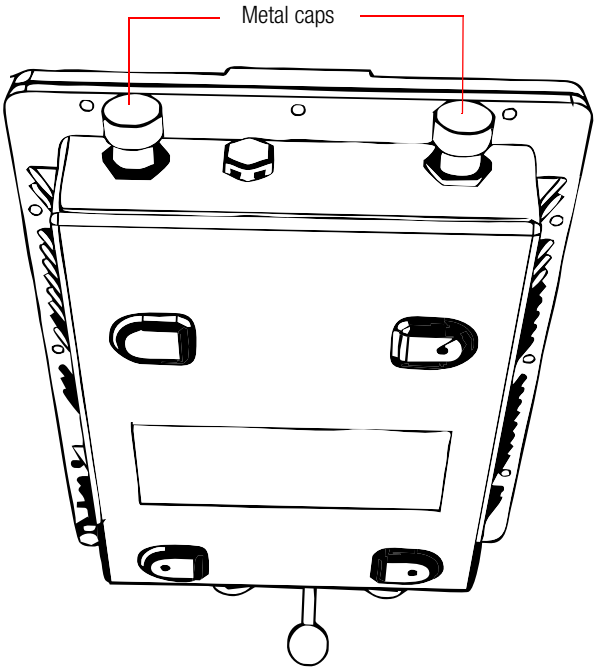
Label	Description
Power LED	• *Off*: No power is available, or the Access Point is not connected to a power source. • *Red: The Access Point is powering on.* • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.

Table 5. LEDs and connectors on the 7762 AP (Continued)

Label	Description
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. *If the Access Point is being managed by Ruckus Wireless ZoneDirector:* • *Green: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.* • *Fast flashing green: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.* • *Slow flashing green: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.* • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point.

If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the Access Point.

Figure 4. The 7762 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-AC Access Point

NOTE ZoneFlex 7762-AC requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 5 and Figure 6 identify the AP external features.

Figure 5. 7762-AC Access Point parts

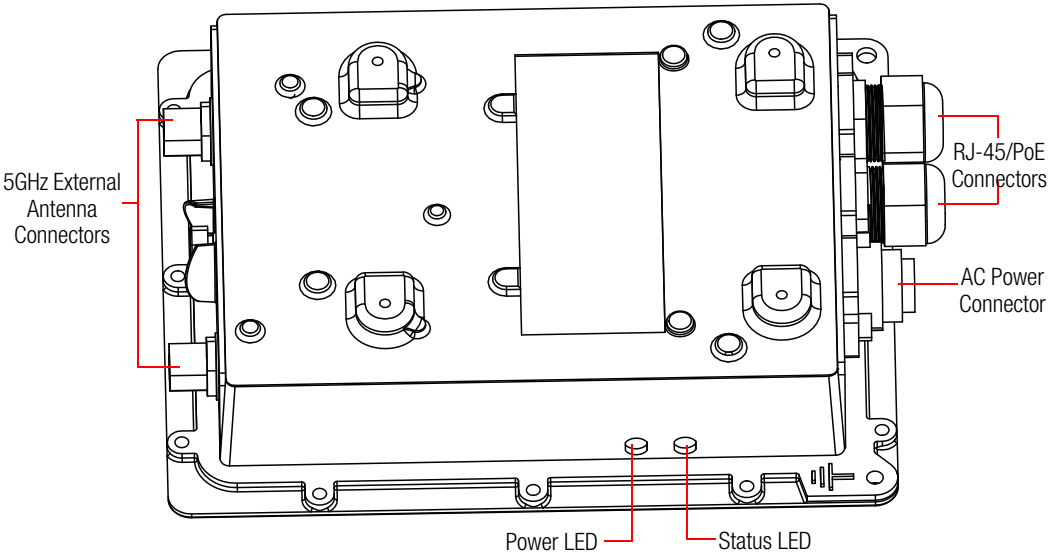


Table 6. LEDs and connectors on the 7762-AC AP

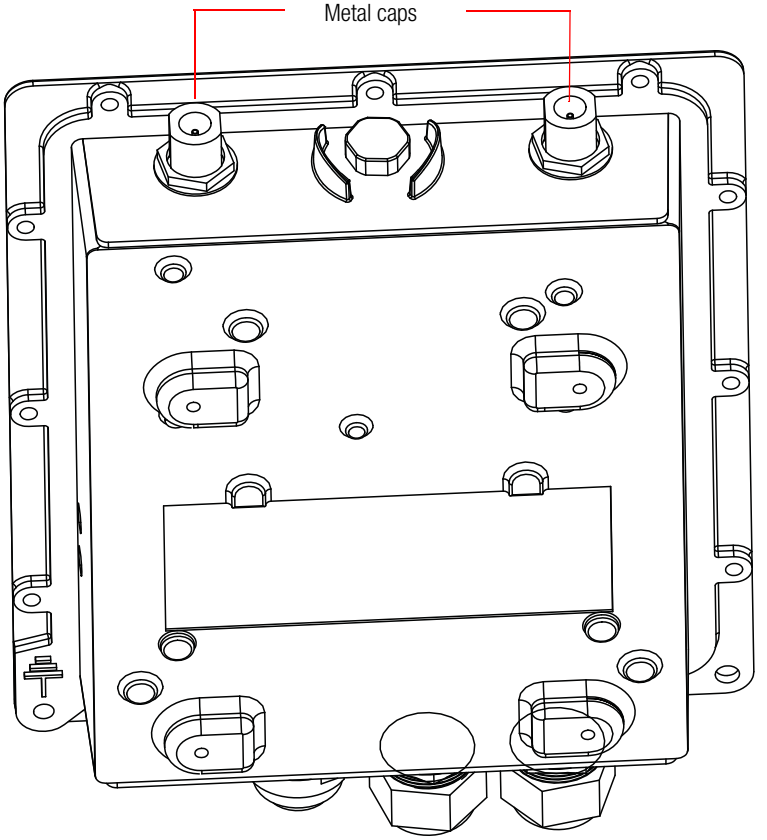
Label	Description
Power LED	• *Off*: No power is available, or the AP is not connected to a power source. • *Red: The AP is powering on.* • *Green*: The AP is connected to a power source and has completed its power-on sequence.

Table 6. LEDs and connectors on the 7762-AC AP (Continued)

Label	Description
Status LED	If the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. *If the AP is being managed by Ruckus Wireless ZoneDirector:* • *Green: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.* • *Fast flashing green: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.* • *Slow flashing green: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.* • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code). • **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.
AC Power Connector	You can use AC to supply power to the AP, in addition to using PoE.

If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 6. The 7762-AC 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-S Access Point

NOTE ZoneFlex 7762-S requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 7 and Figure 8 identify the Access Point external features.

Figure 7. 7762-S Access Point parts

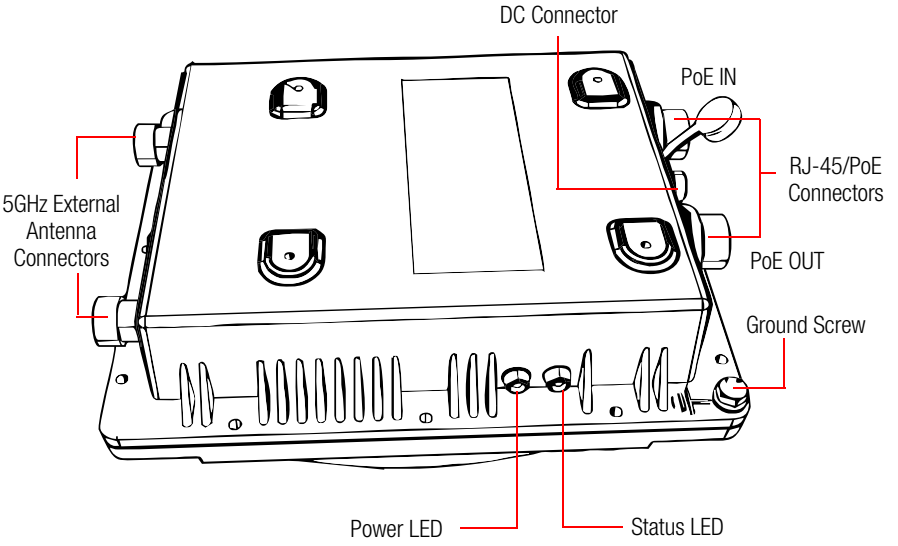


Table 7. LEDs and connectors on the 7762-S Access Point

Label	Description
Power LED	• *Off*: No power is available or the Access Point is not connected to a power source. • *Red: The Access Point is powering on.* • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.

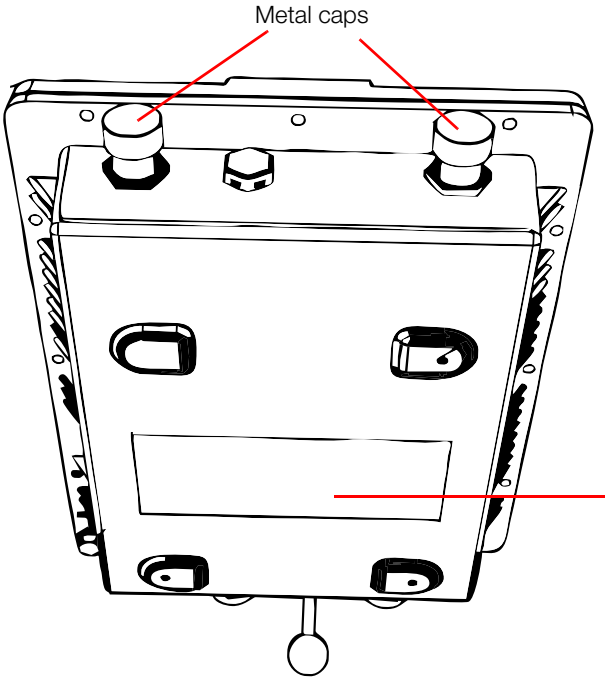
Table 7. LEDs and connectors on the 7762-S Access Point (Continued)

Label	Description
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the Access Point is being managed by Ruckus Wireless ZoneDirector: • *Green:* The AP is part of a mesh network (either as a Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green:* The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with a fair or good signal. • *Slow flashing green:* This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off:* Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point. **NOTE:** *If you connect the Access Point to both PoE and DC power sources at the same time, it uses PoE as the primary power source and DC power as the backup power source.*

7762-S 5GHz Antenna Connectors

If you want to enable the 5GHz sections of the AP (for access or meshing), you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the Access Point.

Figure 8. The 7762-S 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-S-AC Access Point

NOTE ZoneFlex 7762-S-AC requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 9 and Figure 10 identify the AP external features.

Figure 9. 7762-S-AC Access Point parts

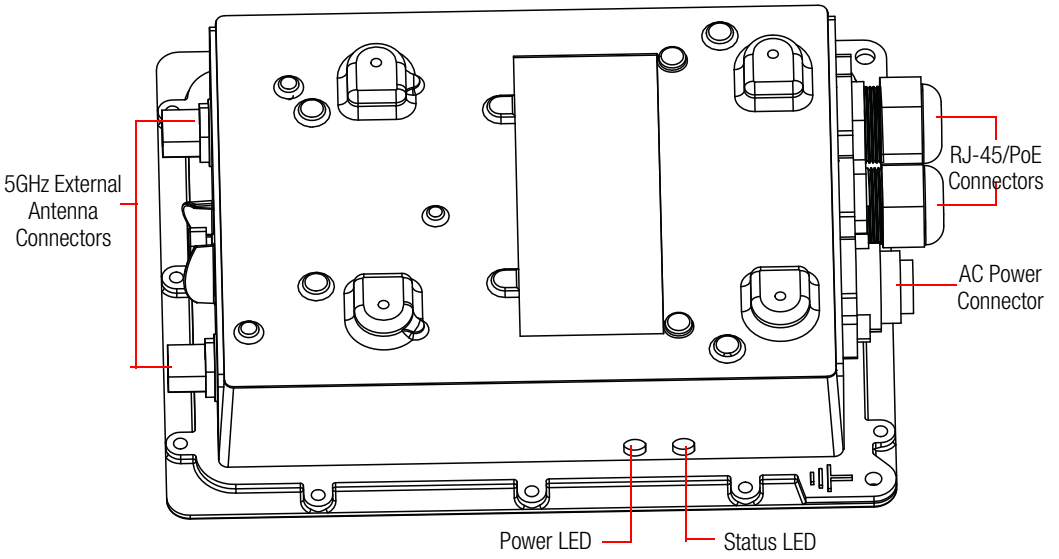


Table 8. LEDs and connectors on the 7762-S-AC AP

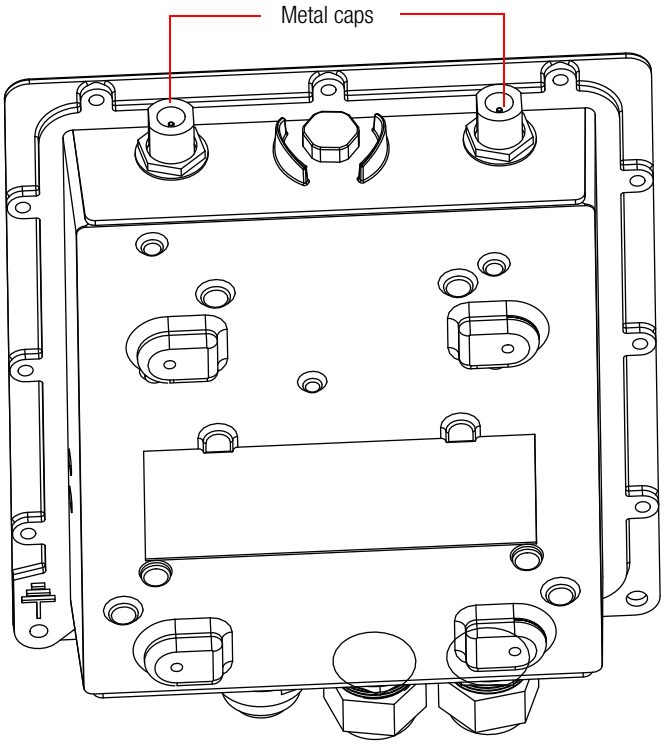
Label	Description
Power LED	• *Off*: No power is available, or the AP is not connected to a power source. • *Red: The AP is powering on.* • *Green*: The AP is connected to a power source and has completed its power-on sequence.

Table 8. LEDs and connectors on the 7762-S-AC AP (Continued)

Label	Description
Status LED	If the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. *If the AP is being managed by Ruckus Wireless ZoneDirector:* • *Green: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.* • *Fast flashing green: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.* • *Slow flashing green: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.* • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code). • **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.
AC Power Connector	You can use AC to supply power to the AP, in addition to using PoE.

If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 10. The 7762-S-AC 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-T Access Point

NOTE ZoneFlex 7762-T requires a minimum of ZoneFlex (ZF) firmware version 9.4 and later to operate.

Figure 11 and Figure 12 identify the Access Point external features.

Figure 11. 7762-T Access Point parts

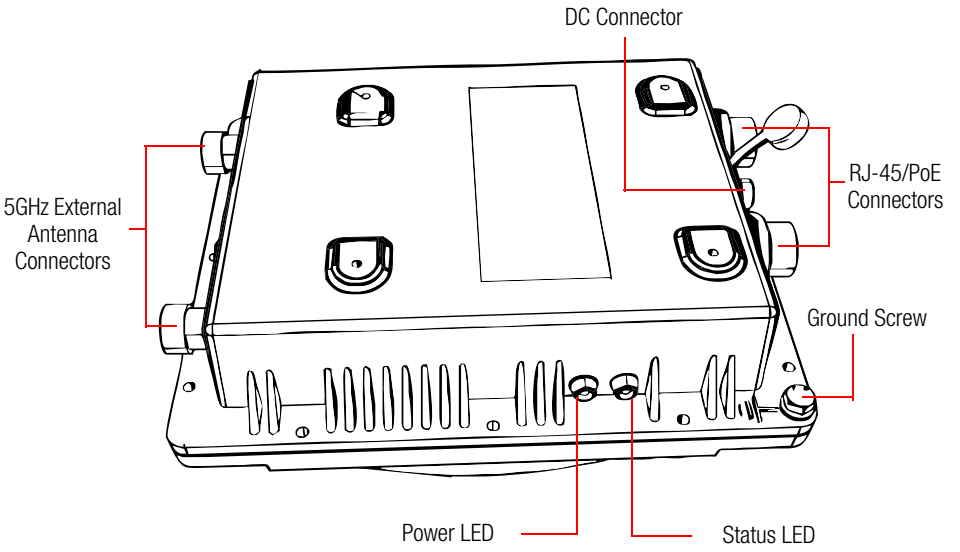


Table 9. LEDs and connectors on the 7762-T AP

Label	Description
Power LED	• *Off*: No power is available, or the Access Point is not connected to a power source. • *Red: The Access Point is powering on.* • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.

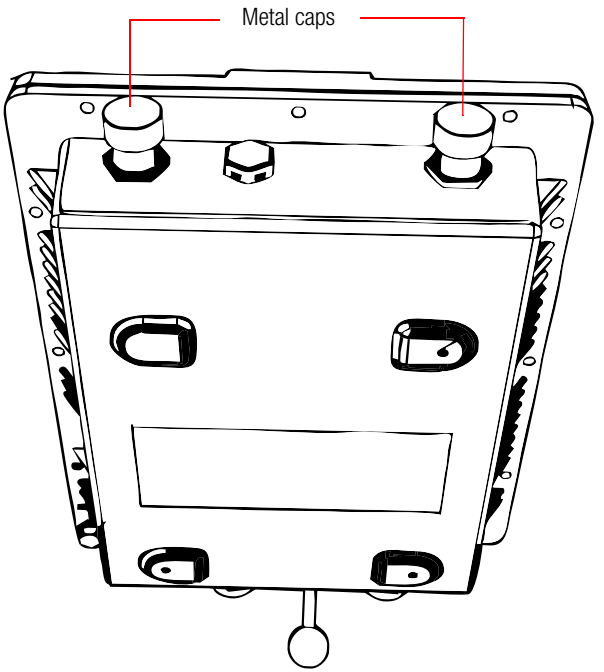
Table 9. LEDs and connectors on the 7762-T AP (Continued)

Label	Description
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the Access Point is being managed by Ruckus Wireless ZoneDirector: • *Green: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.* • *Fast flashing green: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.* • *Slow flashing green: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.* • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point.

If you want to extend the range of your wireless network, you can connect external antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the Access Point.

NOTE The maximum value for the antenna gain that you should set depends on the type of external antennas that you are connecting to the AP.

Figure 12. The 7762-T 5GHz antenna connectors are protected by metal caps



ZoneFlex 7781CM Access Point with Cable Modem

NOTE ZoneFlex 7781CM requires a minimum of ZoneFlex (ZF) firmware version 9.5.1 and later to operate.

Figure 13 and Figure 14 identify the 7781CM AP with integral Cable Modem AP (7781CM) external features.

- The 901-7781-US01 and 901-7781-WW01 DOCSIS 7781CMs and the 901-7781-JP21 JCTEA DOCSIS 7781CMs include a shroud and cable clamps to mount the 7781CMs on strand support cables.
- The 901-7781-WW11 EuroDOCSIS 7781CMs do not include a shroud or cable clamps, and are mounted using customer-supplied mounting brackets.

Figure 13. 7781CM connectors

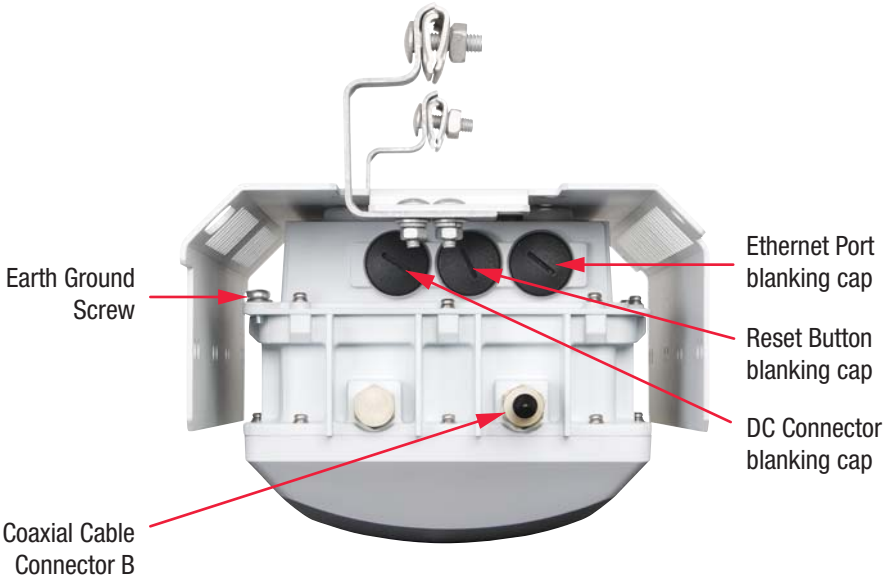


Table 10. Connectors on the 7781CM

Label	Description
Ethernet Port (under blanking cap)	RJ-45 port that supports 10/100/1000Mbps connections and provides 802.3af-compliant (15.4W) Power over Ethernet (PoE) output power to external devices. PoE output (and internal CM heater, if equipped) are only supported when the 7781CM receives Power Over Cable (POC) from the HFC cable plant.
Reset Button (under blanking cap)	Refer to the *ZoneFlex 7781CM Cable Modem Access Point Installation Guide* to access the reset button and either reboot the AP or reset the AP to factory defaults.
DC Connector (under blanking cap)	In addition to the power supplied by the coaxial cable from the cable modem termination system (CMTS) equipment, the 7781CM can also be DC powered for configuration before field deployment.
Coaxial Cable Connector B	Connects to the CMTS at the headend using a tap on the plant, and provides AC POC to the 7781CM. For more information, refer to the *ZoneFlex 7781CM Cable Modem Access Point Installation Guide.*

Figure 14. 7781CM LEDs when the dome is pointing downwards

Reading the 7781CM LEDs

The six dual-purpose LEDs are used both by the CM part and the AP part of the 7781CM:

- When **LED 1** (green LED) is lit, the LEDs are in **Access Point** mode.
- When **LED 2** (white LED) is lit, the LEDs are in **Cable Modem** mode.

While the 7781CM is booting up, the LEDs are in CM mode. Once bootup is completed, the LEDs alternate between CM and AP modes.

NOTE The 7781CM LEDs turn off after a while. This is normal operation.

Refer to the following:

- LED Boot Sequence
- LED Online/Steady State
- Reading LEDs in Access Point Mode
- Reading LEDs in Cable Modem Mode

LED Boot Sequence

1. All LEDs blink for a few seconds.
2. LED 2 (white) stays solid on.
3. LEDs 3, 4, 5 and 6 (blue, middle green, yellow and red) blink in sequence.
4. LEDs 4, 5 and 6 (middle green, yellow and red) blink together for a few seconds.
5. LED 3 (blue) goes solid when the link to the AP is established.
6. LED 6 (red) flashes as CM tries to acquire downstream.
   - LED 6 (red) goes solid when downstream is acquired.
   - LED 3 (blue) flashes to indicate communication across the AP link.
7. LED 5 (yellow) comes on solid when upstream acquired.
8. LED 4 (middle green) on indicates that cable modem came on-line successfully.

LED Online/Steady State

- LED 1 (green) on indicates AP mode.
- LED 2 (white) on indicates CM mode.
- LEDs 3, 4, 5 and 6 (blue, middle green, yellow and red) are on.

The LEDs alternate between CM and AP modes.

NOTE The 7781CM LEDs turn off after a while. This is normal operation.

Reading LEDs in Access Point Mode

In AP mode, **LED 1** (green LED) is lit.

NOTE The LEDs do not indicate whether the AP is in standalone mode or if ZoneDirector is managing the AP. To check if ZoneDirector is managing the access point, log into the ZoneDirector Web interface, go to the Access Points page, and then search for the access point's MAC address. If you are unable to find the access point, then it is very likely in standalone mode. If you have multiple ZoneDirector devices on the network, make sure you check each one of them.

For Cable Operators, APs will typically be in ZoneDirector mode after initial boot. If the AP is unable to reach the ZoneDirector on initial boot, it remains in standalone mode.

Refer to Table 11 for a summary of AP mode LED behavior.

Table 11. LED behavior in AP Standalone and ZoneDirector modes

LED	State	AP Standalone Mode	AP ZoneDirector Mode
1	Solid Green	**On = AP Mode.**	**On = AP Mode.**
2	OFF	Off = Not AP Mode.	Off = Not AP Mode.
3	Solid Blue	At least one 5GHz wireless client is associated with the access point and signal strength is weak.	If AP is RAP, at least one MAP is associated. If AP is MAP it is associated with a RAP. Signal strength is weak.
4	Flashing Green	5GHz WLAN is up but no clients.	5GHz WLAN is up but no clients.
	Solid Green	At least one 5GHz wireless client is associated with the access point and signal strength is strong.	If AP is RAP, at least one MAP is associated. If AP is MAP it is associated with a RAP. Signal strength is strong.
5	Solid Yellow	At least one 2.4GHz wireless client is associated with the access point and signal strength is weak.	At least one 2.4GHz wireless client is associated with the access point and signal strength is weak.

Table 11. LED behavior in AP Standalone and ZoneDirector modes (Continued)

LED	State	AP Standalone Mode	AP ZoneDirector Mode
6	Flashing Red	2.4GHz WLAN is up but no clients.	2.4GHz WLAN is up but no clients.
	Solid Red	At least one 2.4GHz wireless client is associated with the access point and signal strength is strong.	At least one 2.4GHz wireless client is associated with the access point and signal strength is strong.

Reading LEDs in Cable Modem Mode

In CM mode, **LED 2** (white LED) is always lit. Refer to Table 12 for a summary of CM mode LED behavior. Refer to LED Boot Sequence and LED Online/Steady State for more details.

Table 12. LED behavior in CM mode

LED	State	Meaning
1	OFF	Off = Not CM Mode.
2	Solid White	**On = CM Mode.**
3	Solid Blue	Link
4	Solid Green	On line
5	Solid Yellow	Upstream acquired
6	Flashing Red	Searching for downstream
	Solid Red	Downstream acquired

Powering Options

The 7781CM supports both DC power or AC power over cable (POC). Normally 12 VDC power is only used at the depot or when debugging. 40 to 90 VAC POC is only used when the 7781CM is mounted on a cable strand and powered via an F-type coaxial cable connected to the HFC cable plant.

The customer-ordered 1.5A 12 VDC power supply part number is 902-0169-xxyy, where xx = Country and yy = revision.

NOTE The 7781CM does not provide PoE output or support internal heater operation when powered by 12 VDC.

Cable Modem Heater

The 901-7781-US01, 901-7781-JP21 and 901-7781-WW01 7781CM includes a built-in heater for the cable modem that permits operation at extremely low temperatures. The heater is typically on below -10° C (14° F). The heater is powered by POC only. When the 7781CM is powered by 12 VDC, the heater is disabled.

The 901-7781-WW11 EuroDOCSIS 7781CM does not include a built-in heater.

7781CM Operation

Refer to the *ZoneFlex 7781CM Cable Modem Access Point Installation Guide* for information on Cable Modem configuration and operation.

ZoneFlex 7782 Access Point

NOTE ZoneFlex 7782 requires a minimum of ZoneFlex (ZF) firmware version 9.5.1 and later to operate.

Figure 15 identifies the connectors and LEDs on the 7782 Omni AP. Table 13 describes the LEDs and connectors.

Figure 15. Connectors and LEDs on 7782 AP - bottom view

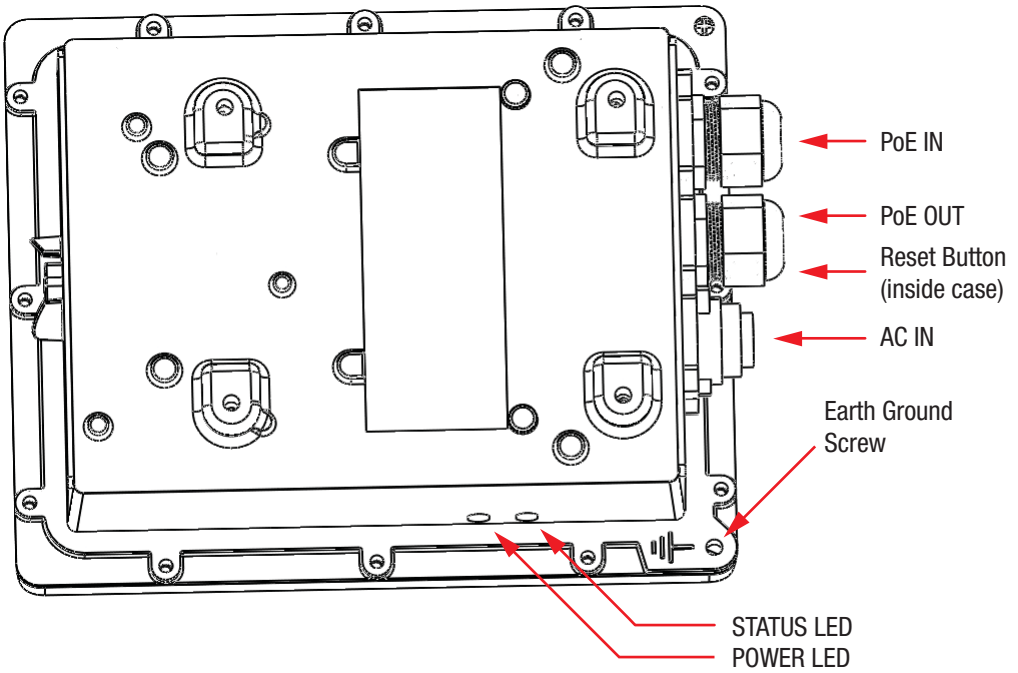


Table 13. 7782 AP LED and connector descriptions

Label	Description
PoE IN RJ45 data connector	Supports 10/100/1000Mbps connections, connects to the network and receives 802.at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.

Table 13. 7782 AP LED and connector descriptions (Continued)

Label	Description
PoE OUT RJ45 data connector	Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (up to 25W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.
Reset button	This button is inside the PoE OUT cable gland. Refer to the *ZoneFlex 7782 Outdoor Access Point Installation Guide* to access the reset button and reset the AP.
AC IN power connector	You can use AC to supply power to the AP, in addition to using PoE.
STATUS LED	When the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. When the AP is being managed by Ruckus Wireless ZoneDirector: • *Green:* The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green:* The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green:* This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off:* Mesh networking is disabled and the WLAN service is unavailable.
POWER LED	• *Off:* No power is available, or the AP is not connected to a power source. • *Red:* The AP is powering on. • *Green:* The AP is connected to a power source and has completed its power-on sequence.

ZoneFlex 7782-E Access Point

NOTE ZoneFlex 7782-E requires a minimum of ZoneFlex (ZF) firmware version 9.5.1 and later to operate.

Figure 16 identifies the connectors and LEDs on the bottom of the 7782-E External Antenna AP. Figure 17 identifies the connectors on the top of the 7782-E.

Figure 16. Connectors and LEDs on 7782-E AP - bottom view

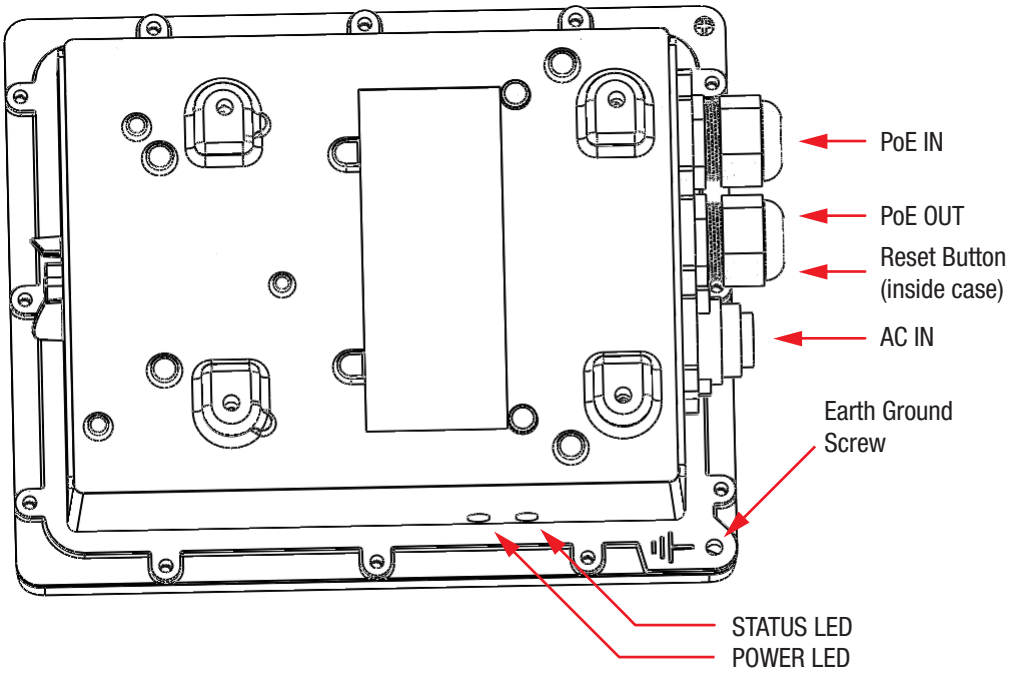


Figure 17. 7782-E access point top-panel N-type connectors

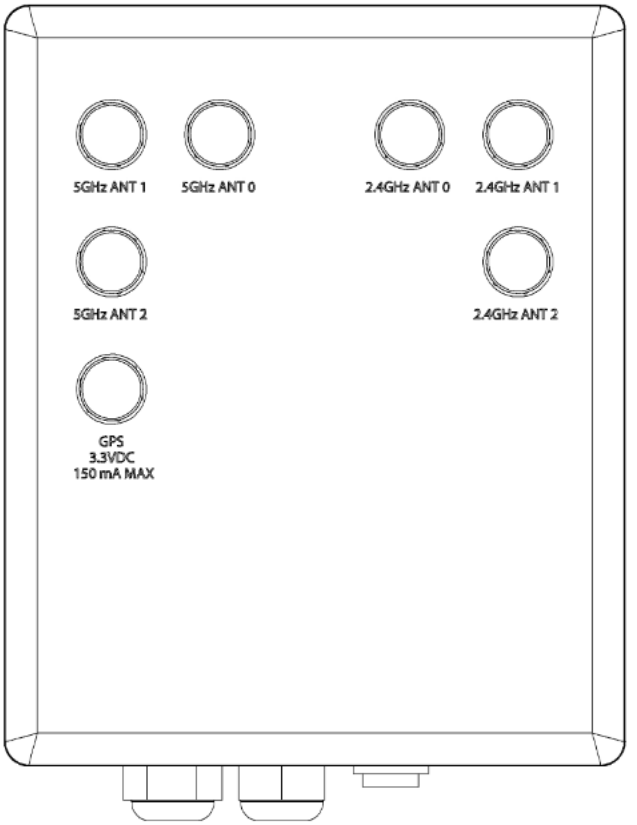


Table 14. Top-panel N-type connectors on the 7782-E access point

Label	Description
5GHz connectors: ANT 0, ANT 1 and ANT 2	These 5GHz 50-ohm female connectors can be used with up to three external antennas for operator-defined coverage areas and point-to-point deployments. • When you are connecting two 5GHz antennas to the AP, use the ANT 0 and ANT 2 5GHz connectors. • When you are connecting three 5GHz antennas to the AP, use the all three ANT 0, ANT 1 and ANT 2 5GHz connectors.

Table 14. Top-panel N-type connectors on the 7782-E access point (Continued)

Label	Description
2.4GHz connectors: ANT 0, ANT 1 and ANT 2	These 2.4GHz 50-ohm female connectors can be used with up to three external antennas for operator-defined coverage areas and point-to-point deployments. • When you are connecting two 2.4GHz antennas to the AP, use the ANT 0 and ANT 2 2.4GHz connectors. • When you are connecting three 2.4GHz antennas to the AP, use the all three ANT 0, ANT 1 and ANT 2 2.4GHz connectors.
GPS connector	This 50-ohm female N-type connector is used for a standard powered external GPS antenna. The factory-supplied GPS antenna kit complies with all 7782-E AP requirements. If you are installing a customer-supplied antenna and extension cable, then keep the cable short or use low-loss cable to avoid excess signal attenuation. The 7782-E supplies 3.3 VDC to the GPS antenna; make sure that a customer-supplied GPS antenna does not require more than 150mA.

ZoneFlex 7782-N Access Point

NOTE ZoneFlex 7782-N requires a minimum of ZoneFlex (ZF) firmware version 9.5.1 and later to operate.

Figure 18 identifies the connectors and LEDs on the 7782-N 30-Degree Narrow Sector AP. Table 15 describes the LEDs and connectors.

Figure 18. Connectors and LEDs on 7782-N AP - bottom view

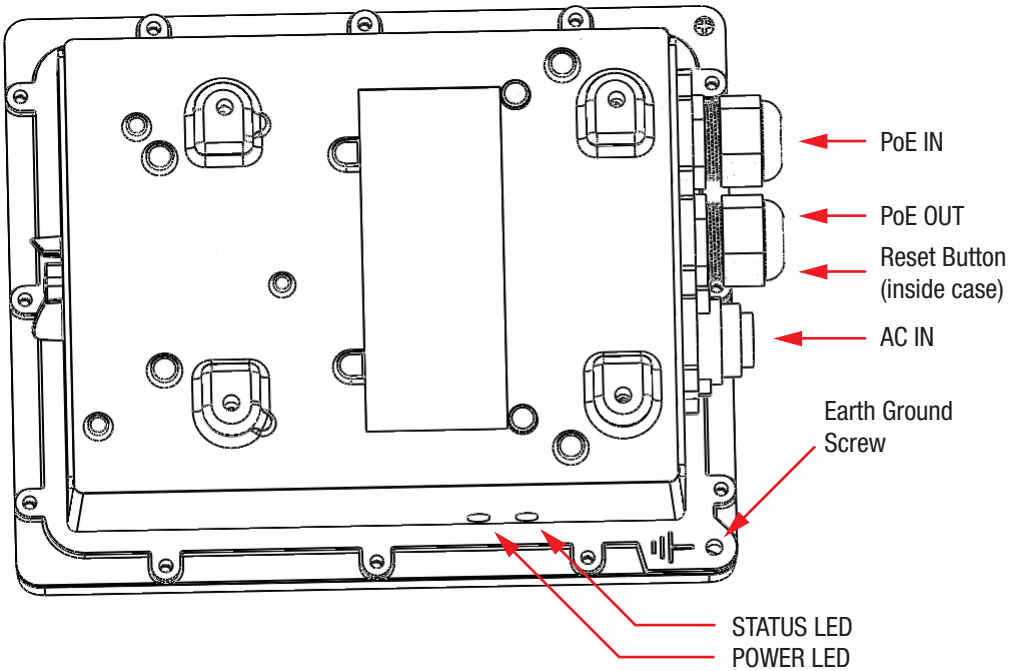


Table 15. 7782-N AP LED and connector descriptions

Label	Description
PoE IN RJ45 data connector	Supports 10/100/1000Mbps connections, connects to the network and receives 802.at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.

Table 15. 7782-N AP LED and connector descriptions (Continued)

Label	Description
PoE OUT RJ45 data connector	Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.
Reset button	This button is inside the PoE OUT cable gland. Refer to the *ZoneFlex 7782 Outdoor Access Point Installation Guide* to access the reset button and reset the AP.
AC IN power connector	You can use AC to supply power to the AP, in addition to using PoE.
STATUS LED	When the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. When the AP is being managed by Ruckus Wireless ZoneDirector: • *Green:* The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green:* The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green:* This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off:* Mesh networking is disabled and the WLAN service is unavailable.
POWER LED	• *Off:* No power is available, or the AP is not connected to a power source. • *Red:* The AP is powering on. • *Green:* The AP is connected to a power source and has completed its power-on sequence.

ZoneFlex 7782-S Access Point

NOTE ZoneFlex 7782-S requires a minimum of ZoneFlex (ZF) firmware version 9.5.1 and later to operate.

Figure 19 identifies the connectors and LEDs on the 7782-S 120-Degree Sector AP. Table 16 describes the LEDs and connectors.

Figure 19. Connectors and LEDs on 7782-S AP - bottom view

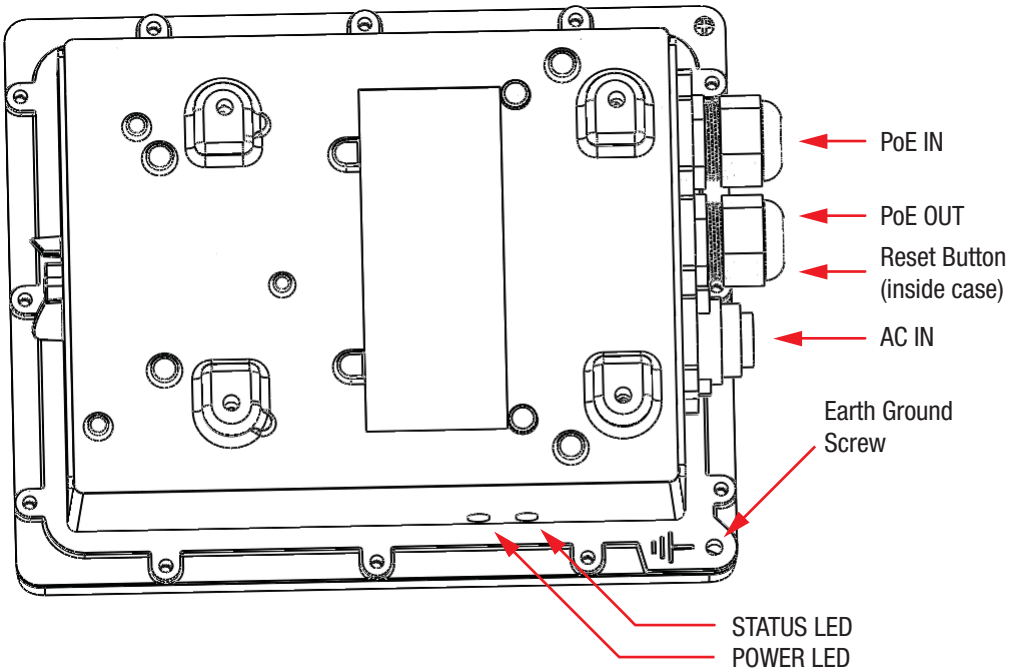


Table 16. 7782-S AP LED and connector descriptions

Label	Description
PoE IN RJ45 data connector	Supports 10/100/1000Mbps connections, connects to the network and receives 802.at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.

Table 16. 7782-S AP LED and connector descriptions (Continued)

Label	Description
PoE OUT RJ45 data connector	Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.
Reset button	This button is inside the PoE OUT cable gland. Refer to the *ZoneFlex 7782 Outdoor Access Point Installation Guide* to access the reset button and reset the AP.
AC IN power connector	You can use AC to supply power to the AP, in addition to using PoE.
STATUS LED	When the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. When the AP is being managed by Ruckus Wireless ZoneDirector: • *Green:* The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green:* The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green:* This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off:* Mesh networking is disabled and the WLAN service is unavailable.
POWER LED	• *Off:* No power is available, or the AP is not connected to a power source. • *Red:* The AP is powering on. • *Green:* The AP is connected to a power source and has completed its power-on sequence.

SmartCell SC8800-S Outdoor Access Point

CAUTION! SmartCell SC8800-S requires a minimum of ZoneFlex (ZF) firmware version 9.6.1 and later to operate. **DO NOT CONNECT THE SC8800-S TO A RUCKUS WIRELESS CONTROLLER WITH ZF 9.6.0 OR EARLIER.**

Figure 20 identifies the top-panel connectors on the AP. Table 17 describes these connectors.

Figure 20. Top-panel connectors

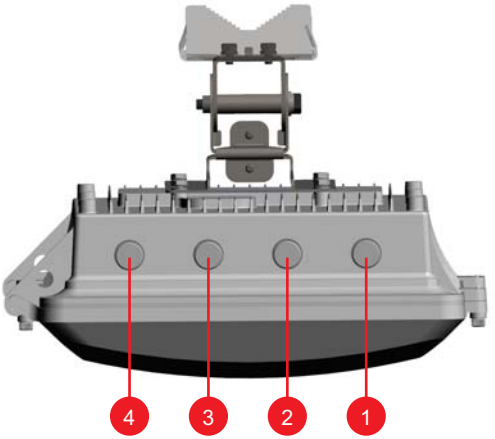


Table 17. Top-panel connectors

No.	Label	Description
1	**5 GHz ANT 0** port	5GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.
2	**2.4 GHz ANT 2** port	2.4GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.
3	**2.4 GHz ANT 0** port	2.4GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.
4	**5 GHz ANT 2** port	5GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.

Figure 21 identifies the AP bottom-panel connectors and LED locations on the AP. Table 18 describes these connectors and LEDs.

Figure 21. Bottom-panel connectors and LED locations

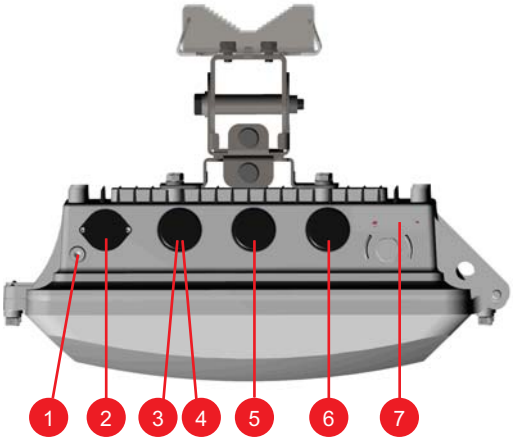


Table 18. Bottom-panel connectors

No.	Label	Description
1	Earth ground screw	Use this screw to attach an earth ground to the AP as required by local regulations.
2	**AC** power connector	You can use AC to supply power to the AP, in addition to using PoE.
3	**PoE OUT** RJ45 data connector	Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, an IP-based surveillance camera). This port alternatively can supply 802.3at (25.5W) PoE when used with 20m (65.6 ft.) or shorter CAT5e UTP or better cable.
4	**RESET** button	This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE OUT** RJ-45 waterproof gland.
5	**PoE IN** RJ45 data connector	Supports 10/100/1000Mbps connections, connects to the network and receives Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.

Table 18. Bottom-panel connectors (Continued)

No.	Label	Description
6	**FIBER** port	This waterproof gland allows you to run a fiber-optic cable into the SC8800-S chassis to an optional fiber modem.
7	LEDs	See Figure 22.

Figure 22 identifies the AP bottom-panel LED locations on the AP. Table 19 describes these connectors and LEDs.

Figure 22. LEDs

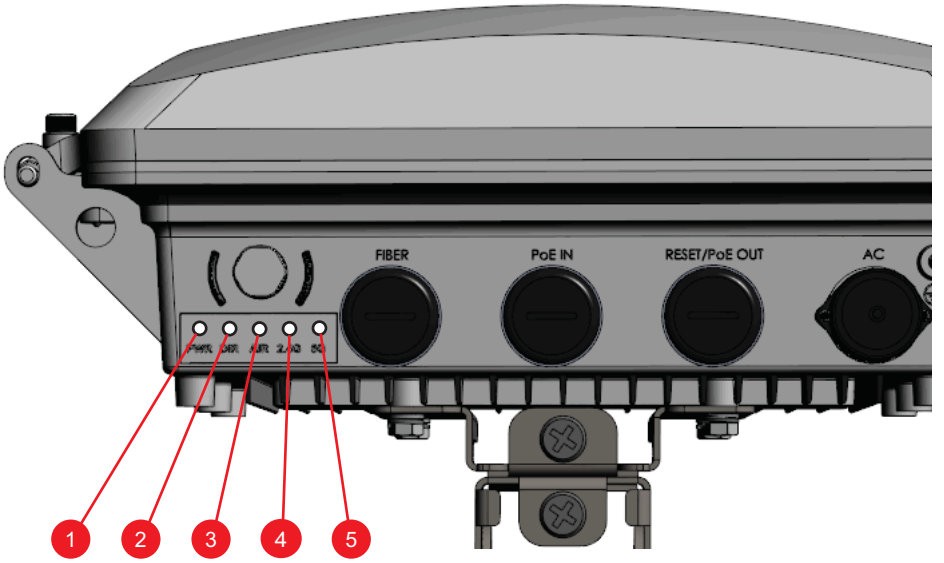


Table 19. LED descriptions

No.	Label	Description
1	**PWR** LED	• *Off:* No power is available, or the AP is not connected to a power source. • *Solid Red:* The AP is powering on. • *Solid Green:* The AP is connected to a power source and has completed its power-on sequence.

Table 19. LED descriptions (Continued)

No.	Label	Description
2	**DIR** LED	• *Off:* The AP is NOT managed by ZoneDirector (standalone mode). • *Solid Green:* The AP is managed by ZoneDirector and connection to ZoneDirector has been established. • *Fast Flashing Green (twice per second):* The AP is managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update. • *Slow Flashing Green (once every two seconds):* The AP is managed by ZoneDirector, but is currently unable to communicate with ZoneDirector.
3	**AIR** LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Solid Green:* The AP is functioning as a Mesh AP (MAP) and the uplink signal quality is good (>24dBm). • *Fast Flashing Green (twice per second):* The AP is functioning as a Mesh AP (MAP) and the wireless signal to its uplink AP is fair. • *Slow Flashing Green (once every two seconds):* The AP is in mesh mode, but the AP is still searching for a mesh uplink.
4	**2.4G** LED	• *Off:* WLAN service is down. • *Amber (Yellow):* WLAN service is up but with no client connected. • *Solid Green:* WLAN service is up with at least one client connected.

Table 19. LED descriptions (Continued)

No.	Label	Description
5	**5G** LED	• *Off:* WLAN service is down. • *Amber (Yellow):* WLAN service is up but with no clients or downlink MAPs associated/connected. • *Solid Green:* WLAN service is up with at least one client is associated. No downlink MAPs are connected. • *Fast Flashing Green (twice per second):* The WLAN is up, at least one downlink MAP is connected, and at least one client is associated. • *Slow Flashing Green (once every two seconds):* The WLAN is up and at least one downlink MAP is connected. No clients are associated.

T300 Outdoor Access Point

CAUTION! The minimum software revision for the T300 AP is ZoneFlex (ZF) 9.8.1, or SmartCell Gateway (SCG) 2.5.1 or later.

Do not connect the T300 AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.

Figure 23 identifies the LEDs and connectors on the AP. Table 20 describes these LEDs and other elements.

Figure 23. LEDs and other elements

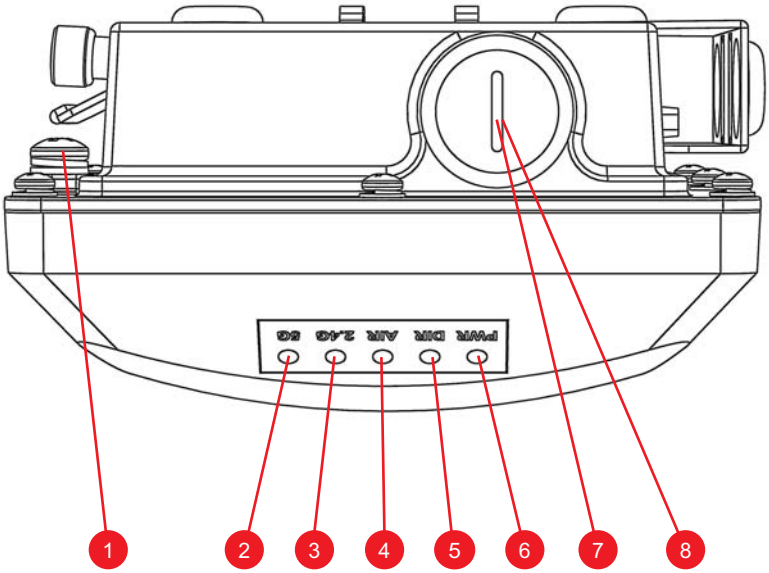


Table 20. LED and other element descriptions

No.	Label	Description
1	Earth ground screw	Use this screw to attach an earth ground to the AP as required by local regulations.

Table 20. LED and other element descriptions (Continued)

No.	Label	Description
2	**5G** LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated. **Note:** *The mesh (RAP and MAP) functions are available on the T300 in a future release.*
3	**2.4G** LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.
4	**AIR** LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink. **Note:** *The mesh (RAP and MAP) functions are available on the T300 in a future release.*

Table 20. LED and other element descriptions (Continued)

No.	Label	Description
5	**DIR** LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
6	**PWR** LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
7	**PoE IN** RJ45 data connector	Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE). **Note:** *The T300 can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T300 data sheet for recommended PoE accessories.*
8	**RESET** button	This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE IN** RJ-45 waterproof gland.

T301n Outdoor Access Point

CAUTION! The minimum software revision for the T301n AP is ZoneFlex (ZF) 9.8.1, or SmartCell Gateway (SCG) 2.5.1 or later.

Do not connect the T301n AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.

Figure 24 identifies the LEDs and connectors on the AP. Table 21 describes these LEDs and other elements.

Figure 24. LEDs and other elements

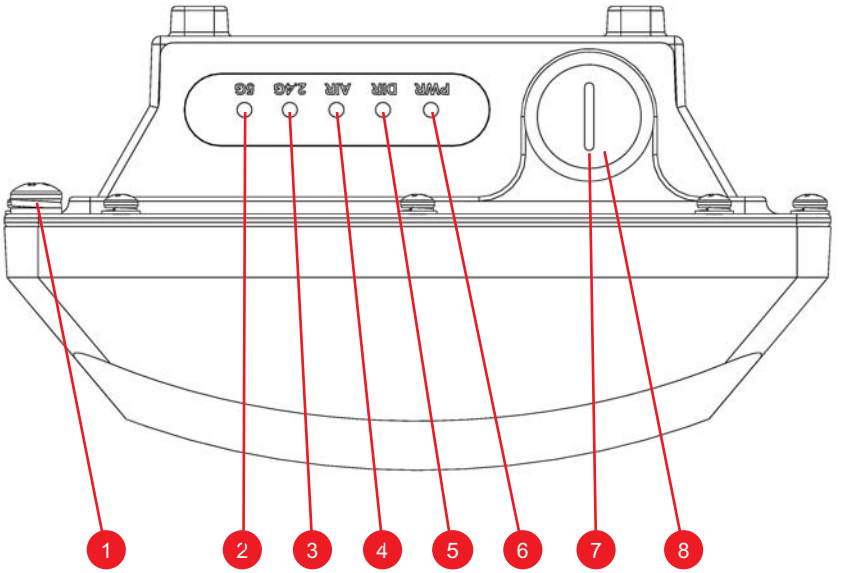


Table 21. LED and other element descriptions

No.	Label	Description
1	Earth ground screw	Use this screw to attach an earth ground to the AP as required by local regulations.

Table 21. LED and other element descriptions (Continued)

No.	Label	Description
2	**5G** LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated. **Note:** *The mesh (RAP and MAP) functions are available on the T301n in a future release.*
3	**2.4G** LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.
4	**AIR** LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink. **Note:** *The mesh (RAP and MAP) functions are available on the T301n in a future release.*

Table 21. LED and other element descriptions (Continued)

No.	Label	Description
5	**DIR** LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
6	**PWR** LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
7	**PoE IN** RJ45 data connector	Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE). **Note:** *The T301n can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T301n data sheet for recommended PoE accessories.*
8	**RESET** button	This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE IN** RJ-45 waterproof gland.

T301s Outdoor Access Point

CAUTION! The minimum software revision for the T301s AP is ZoneFlex (ZF) 9.8.1, or SmartCell Gateway (SCG) 2.5.1 or later.

Do not connect the T301s AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.

Figure 25 identifies the LEDs and connectors on the AP. Table 22 describes these LEDs and other elements.

Figure 25. LEDs and other elements

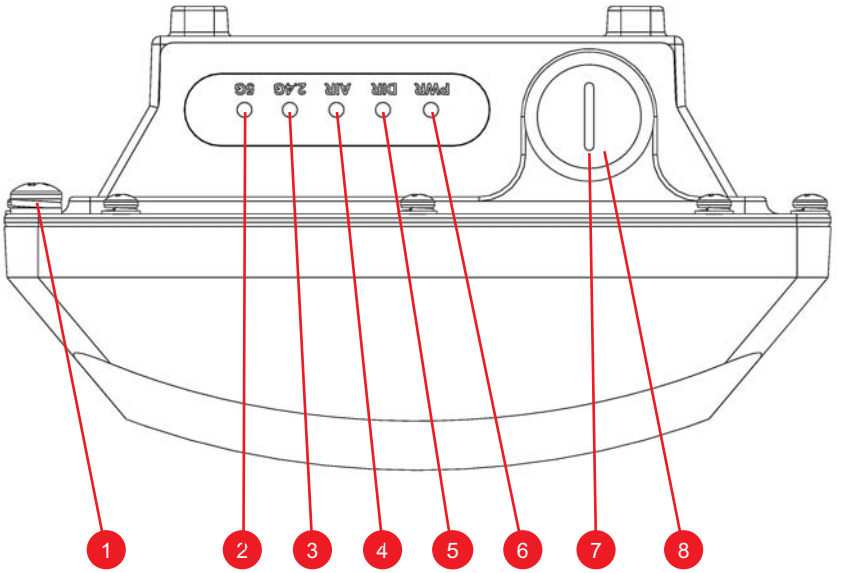


Table 22. LED and other element descriptions

No.	Label	Description
1	Earth ground screw	Use this screw to attach an earth ground to the AP as required by local regulations.

Table 22. LED and other element descriptions (Continued)

No.	Label	Description
2	**5G** LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated. **Note:** *The mesh (RAP and MAP) functions are available on the T301s in a future release.*
3	**2.4G** LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.
4	**AIR** LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink. **Note:** *The mesh (RAP and MAP) functions are available on the T301s in a future release.*

Table 22. LED and other element descriptions (Continued)

No.	Label	Description
5	**DIR** LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.
6	**PWR** LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
7	**PoE IN** RJ45 data connector	Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE). **Note:** *The T301s can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T301s data sheet for recommended PoE accessories.*
8	**RESET** button	This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE IN** RJ-45 waterproof gland.

Navigating the Web Interface

2

In this chapter:

- Logging Into the ZoneFlex AP Web Interface
- Navigating the Web Interface
- When Using a Dual-Band Access Point

Logging Into the ZoneFlex AP Web Interface

You can manage your AP with the ZoneFlex Web interface (which you already used to configure basic AP parameters). If your ZoneFlex network is managed by a Ruckus Wireless ZoneDirector, then you can manage APs using ZoneDirector rather than individually logging into each AP's Web interface.

NOTE The following procedure assumes that you know the static IP address of the AP (now in use), or you have some means of determining the dynamic IP address in use by the AP. The PC you use for AP administration should be on the management VLAN, if VLANs are used in your network.

Refer to the outdoor access point installation guide for instructions on how to connect an administrative computer to the AP.

---

1. On the PC, open a Web browser window.
2. In the address or location bar, type the IP address of the AP. Default IP address for standalone ZoneFlex APs:

   `192.168.0.1` (or **`192.168.100.2`** for Cable Modem APs)
3. Press `<Enter>` to connect to the Web interface.
4. If a Windows security alert dialog box appears, then click **Yes** or **OK** or **Proceed anyway** (depending on the browser) to continue. The Ruckus Wireless Admin login page appears.
5. In *Username*, type **`super`**.
6. In *Password*, type **`sp-admin`**.
7. Click **Login**.

The ZoneFlex Access Point Web interface appears.

Navigating the Web Interface

You manage the Access Point through a Web browser-based interface that you can access from any networked computer. Table 23 lists the Web interface features that are identified in Figure 26.

Figure 26. Elements of the ZoneFlex AP Web Interface

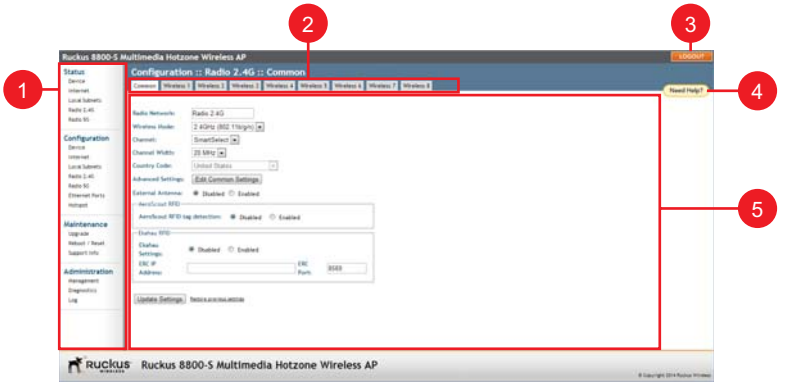


Table 23. ZoneFlex AP Web interface elements

No.	Element	Description
1	Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
2	Tabs	Contains additional options for the configuration page. For example, the **Configuration** > **Wireless** page includes one tab for common wireless configuration and eight tabs for each of the WLANs for the selected radio.
3	LOGOUT Button	Click this button to log out of the AP.
4	Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.
5	Workspace	This large area displays features, options and indicators relevant to your menu bar choices.

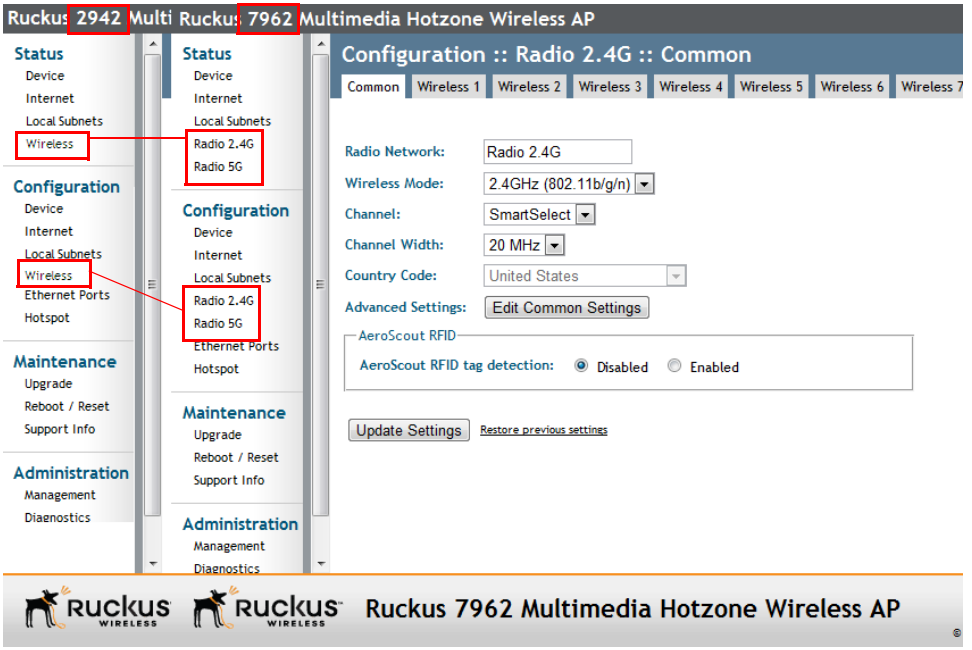
When Using a Dual-Band Access Point

If your ZoneFlex AP model is dual-band, then note that elements on the Web interface menu are slightly different from single-band ZoneFlex AP models.

Dual-band ZoneFlex APs have one 2.4GHz radio (for 802.11b/g/n clients) and one 5GHz radio (for 802.11a/n clients). The wireless settings for these two radios need to be configured separately, which is why the dual-band AP Web interface has the **Radio 2.4G** and **Radio 5G** menu items, instead of a single **Wireless** menu item in single-band models.

Figure 27 highlights the differences between single-band and dual-band ZoneFlex AP menus.

Figure 27. Menu items are slightly different in single-band APs (left) and dual-band ZoneFlex AP models (right)



Configuring the Access Point 3

In this chapter:

- Configuring Device Settings
- Configuring Internet Settings
- Configuring Local Subnets
- Configuring Wireless Settings
- Configuring Ethernet Ports
- Configuring Hotspot Service

This chapter provides instructions for configuring ZoneFlex Access Points in a standalone configuration. If you plan to manage your ZoneFlex network using ZoneDirector, refer to the *ZoneDirector User Manual,* available from the Ruckus website at

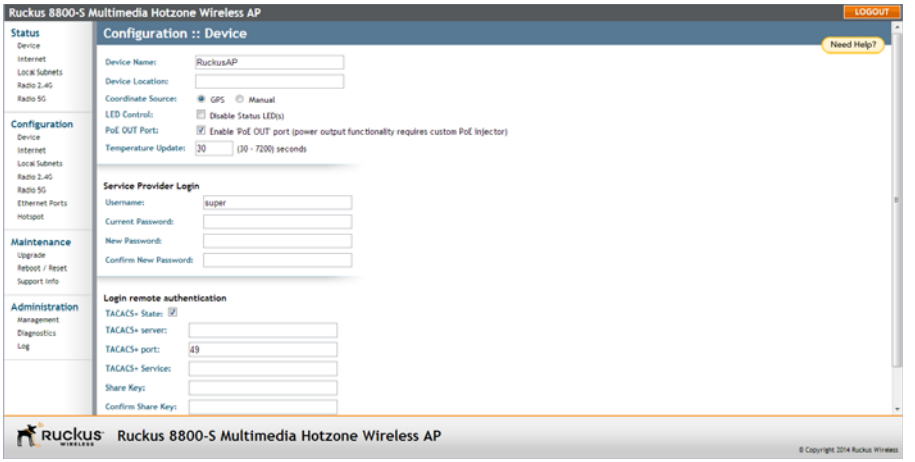
http://support.ruckuswireless.com/documents.

Configuring Device Settings

Device settings refer to the device name, location, temperature update, service provider login, and other settings. (Some settings are only available on certain ZoneFlex models.)

1 Go to **Configuration** > **Device**.

Figure 28. The Configuration > Device page



2 In *Device Name,* type a new name for the device or leave as is to accept the default device name (`RuckusAP`). The device name identifies this access point among other devices on the network.

3 Configure the following optional settings as desired:

- Enter *Device Location* to keep track of the physical location of the AP.
- If the AP has a GPS antenna, then select the method of entering the GPS coordinates. In *Coordinate Source,* select **GPS** to have the GPS antenna automatically determine and enter the GPS coordinates, or select **Manual** to enter the GPS coordinates manually.

  If you selected **Manual**, then enter *GPS Coordinates* to record the physical location of the AP.
- Under *LED Control* (specific models only), check the *Disable Status LED(s)* box to turn off the status LEDs. This can be useful when the AP is installed in a public location, to avoid drawing attention to the AP.
- Enable *Internal Heater* and *PoE OUT Port* (specific models only) if needed.

- In *Temperature Update* (specific models only), enter the interval (in seconds) to report the internal temperature of the device.

4 Under *Service Provider Login,* change the login information as required:

- *Username:* Type the name that you want to use for logging into the Web interface. The default user name is `super`.
- *Current Password:* When you are changing the password, enter the existing password here.
- *New Password:* When you are changing the password, enter the new password The default password is `sp-admin`. The password must consist of six to 32 alphanumeric characters only.
- *Confirm New Password:* Retype the new password to confirm.

5 Under *Login remote authentication,* click the *TACACS+ State* box to enable the TACACS+ server interface, if required.

NOTE Terminal Access Controller Access-Control System Plus (TACACS+) is an AAA protocol used to authenticate administrator login to this device. Users can be authenticated/authorized to monitor, operate or configure this device. Default is disabled. Administrators can be assigned any of the following three administration privilege levels:

- *Super Admin* (Perform all configuration and management tasks)
- *Operator Admin* (Change settings affecting single APs only)
- *Monitoring Admin* (Monitoring and viewing operation status only)

If the TACACS+ server state is enabled, then configure the TACACS+ server parameters:

- *TACACS+ server*: IPv4 or IPv6 server address.
- *TACACS+ port*: 49 is the default, but it can be set to any available TCP port.
- *TACACS+ Service*: Login name.
- *Share Key*: TACACS+ Password.
- *Confirm Share Key*: retype the TACACS+ Password.

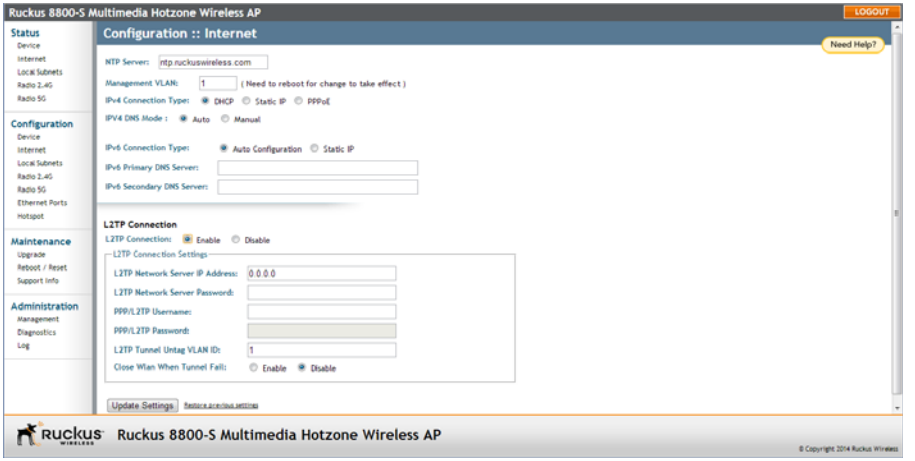
6 Click **Update Settings** to save and apply your changes.

Configuring Internet Settings

Internet settings define how the Access Point connects to your local area network and to the Internet. This section describes how to view and configure the Access Point's Internet settings. Topics discussed include:

- VLAN Settings Overview
- Configuring an NTP Server
- Configuring the Management VLAN
- Default IP Addressing Behavior
- Obtaining and Assigning an IP Address
- Configuring L2TP Connection Settings

Figure 29. The Configuration > Internet page



VLAN Settings Overview

A Ruckus Wireless access point is like a network switch, in that it supports Wi-Fi connections. As such, like many advanced switches, Ruckus APs conform to the IEEE 802.1Q standard -- the standard that defines virtual LANs. In an 802.1Q switch, the concept of VLANs is always present. If a packet arrives without an 802.1Q header, it is assigned to the *native VLAN* or *untag VLAN.*

Each of the AP's wireless interfaces can be assigned a single VLAN. When a packet enters the AP through its wireless interface, the packet is assigned to the Access VLAN configured on the *Configuration* > *Wireless* page (by default, 1).

AP Ethernet ports however, can be configured to pass all VLAN traffic (Trunk Ports) or multiple specific VLANs (General ports).

The VLAN displayed in the Web interface shows the AP's view of the VLAN environment; when a packet arrives at an AP's Ethernet port, the port's VLAN configuration helps determine if the packet is accepted or not (VLAN membership), and assigns a default VLAN (untagged VLAN) if the packet contains no 802.1Q header.

In general, if your network has VLANs deployed already, you should apply VLAN configuration to Ruckus APs so that the configuration across the network is consistent.

Configuring an NTP Server

A network time protocol (NTP) server should be configured to ensure that the Access Point maintains the correct time. The default Ruckus Wireless NTP Server (*ntp.ruckuswireless.com*) can be used if you do not have an NTP server on your network.

If you want the AP to use a different NTP server, you can do so by going to **Configuration > Internet**, entering the host name in *NTP Server* at the top of the page, and then clicking **Update Settings**.

Configuring the Management VLAN

NOTE Changing the Management VLAN causes you to be immediately disconnected from the Web interface if the computer you are using is not on the same VLAN. Do not change the Management VLAN unless your admin PC is on the same VLAN, or you are disconnected and unable to connect again without factory resetting the AP.

If you want to place this AP's management traffic into a management VLAN, enter the VLAN ID in the *Management VLAN* field and click **Update Settings**.

Default IP Addressing Behavior

By default, the Access Point is configured to automatically obtain an IPv4 address from a DHCP server on the network. If the Access Point does not detect a DHCP server, it automatically assigns itself the static IP address `192.168.0.1` (or `192.168.100.2` for Cable Modem APs) to make it easier for you to configure and deploy it on your network.

For IPv6, the Auto Configuration setting serves the same purpose as DHCP. The default static IPv6 address is `fc00::1`.

Obtaining and Assigning an IP Address

There are three methods of assigning IP addresses to the Access Point:

- DHCP/Auto Configuration
- Configuring a Static IP
- PPPoE

DHCP/Auto Configuration

If you leave the Access Point at its default configuration, then it attempts to obtain an IPv4 address from a DHCP server on the network.

In an IPv6 network environment, the AP attempts to obtain an IPv6 address from an IPv6 Auto Configuration server.

Refer to the following:

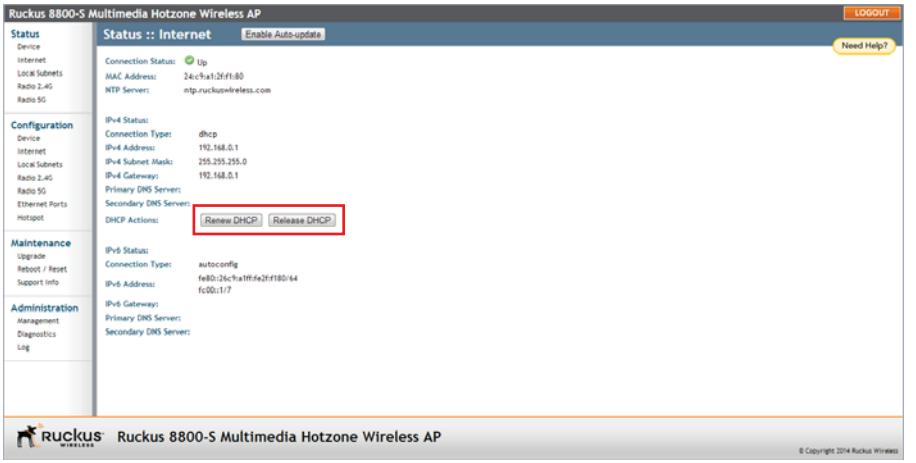
- Renewing and Releasing DHCP
- Configuring IPv4 Auto or Manual Configuration
- Configuring IPv6 Auto Configuration

Renewing and Releasing DHCP

This task should be performed only if you have access to the DHCP server or have some way to determine what IP address has been assigned to the AP. It serves as a troubleshooting technique when IP addresses to one or more networked devices prove to be unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

1 Go to **Status** > **Internet**.

Figure 30. Renew or Release DHCP



2 Review the current settings.

3 If the current *Connection Type* is **dhcp**, then you are able to see the currently-assigned IP address and subnet mask listed below.

- To force the AP to release its DHCP-assigned IP address, click **Release DHCP**. This disconnects the user from Web interface as the system reverts to its default IP address. Log in to the device using the default IP address (**`192.168.0.1`** (or **`192.168.100.2`** for Cable Modem APs) and click **Renew DHCP** to request a new lease from the DHCP server.
- Click **Renew DHCP** to request a new IP address lease from the DHCP server. *Note: The IP address may or may not change depending on the lease time offered to this device.*

4 Click **Update Settings** to save your changes.

Configuring IPv4 Auto or Manual Configuration

If you leave the Access Point at its default configuration, it attempts to obtain an IPv4 address from a DHCP server on the network.

1 Go to **Configuration > Internet**.

2 In *IPv4 Connection Type*, select **DHCP.**

3 In *IPv4 DNS Mode*, select **Auto** or **Manual**.

- When you select *Auto*, the AP automatically searches for an IPv4 DNS server.
- When you select *Manual*, also make the following entries:

- *IPv4 Primary DNS Server:* The IP address of the primary Domain Name System (DNS) server.
- *IPv4 Secondary DNS Server:* The IP address of the secondary DNS server.

4 Click **Update Settings** to save your changes

Configuring IPv6 Auto Configuration

In an IPv6 network environment, the AP attempts to obtain an IPv6 address from an IPv6 Auto Configuration server.

1 Go to **Configuration > Internet**.
2 In *IPv6 Connection Type*, select **Auto Configuration.**
3 In *IPv6 Primary DNS Server*, enter the IP address of the primary IPv6 DNS server.
4 In *IPv6 Secondary DNS Server*, enter the IP address of the secondary IPv6 DNS server.
5 Click **Update Settings** to save your changes

Configuring a Static IP

There are at least two instances when you need to configure a static IP address for the Access Point:

- If the current IP address that the Access Point is using consistently conflicts with that of another device on the network.
- If you want to switch from DHCP to static IP addressing to manage and maintain the Access Point.

Unless you are able to determine the IP address assigned by the DHCP/Auto Configuration server to the Access Point, it may prove helpful for anyone needing administrative access to assign a static IP address.

1 Go to **Configuration** > **Internet**.

You can configure static addresses for IPv4, IPv6 or both. The AP maintains both sets of IP address settings if both are configured.

2 In *IPv4 Connection Type* or *IPv6 Connection Type*, select **Static IP**.
3 When the *Internet Connection Settings* options appear, you can make changes to the following settings:

- (IPv6 only) *IPv6 Primary DNS Server:* The IP address of the primary IPv6 DNS server.

- (IPv6 only) *IPv6 Secondary DNS Server:* The IP address of the secondary IPv6 DNS server.
- *IPv4/IPv6 Address:* **Enter the static IP address that you want to assign to the AP** in either IPv4 (dot-decimal) or IPv6 (colon-separated) format.
- *IPv4 Subnet Mask* or *IPv6 Prefix Length:* Enter the subnet mask or prefix length for the network.
- *IPv4/IPv6 Gateway:* Enter the gateway IP address of the Internet interface.

4 (IPv4 only) In *IPv4 DNS Mode*, select **Auto** or **Manual**.

- When you select *Auto*, the AP automatically searches for an IPv4 DNS server.
- When you select *Manual*, also make the following entries:
  - *IPv4 Primary DNS Server:* The IP address of the primary DNS server.
  - *IPv4 Secondary DNS Server:* The IP address of the secondary DNS server.

5 Click **Update Settings** to save your changes.

PPPoE

Point to Point Protocol over Ethernet (PPPoE) is a Layer 2 protocol which uses the PPP (Point to Point) protocol to connect a client system to a server system over a one to one network link. All traffic for a PPPoE connected client must go through the PPPoE server to reach the client. A PPPoE server can therefore be used to route, NAT, firewall, and perform QoS traffic shaping.

If a PPPoE server is used to distribute Internet access to subscribers, the Access Point can be configured with a PPPoE username and password to authenticate with the PPPoE server.

PPPoE is available only for the IPv4 connection type; PPPoE is not supported in IPv6 environments.

1 Go to **Configuration > Internet**.

2 Under *IPv4 Connection Type*, select **PPPoE**.

3 Enter a *PPPoE Username.*

4 Enter a *PPPoE Password.*

5 Retype the password in *PPPoE Password Confirmation.*

6 Click **Update Settings** to save your changes.

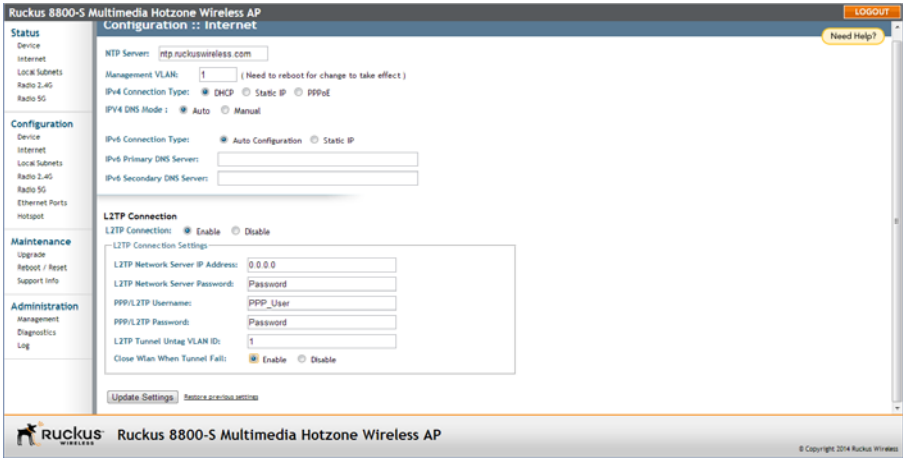
Configuring L2TP Connection Settings

You can implement transparent bridging with ZoneFlex by using L2TP (Layer 2 Tunneling Protocol) tunneling. By tunneling traffic from a ZoneFlex AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials.

In the case of L2TP, the ZoneFlex AP functions as a remote bridge. As such, it forwards traffic into PPP sessions over the L2TP tunnel. This implementation ensures that you have complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed (bridged) onto the ISP's core network.

1 Go to **Configuration** > **Internet**.

Figure 31. L2TP Connection



2 At *L2TP Connection,* click **Enable**.

3 In *L2TP Network Server IP Address,* type the IP address of the L2TP network server (LNS) to which the device connects.

4 In *L2TP Network Server Password,* type the L2TP server password.

5 If your network requires PPP authentication, configure the following fields for L2TP/PPP authentication:

- *PPP/L2TP Username:* Type your PPP user name.
- *PPP/L2TP Password:* Type the password for the account.
- *L2TP Tunnel Untag VLAN ID:* Enter the Untag VLAN ID for the L2TP tunnel.

6 In *Close WLAN When Tunnel Fail,* select **Enable** if you want to disable the WLAN when the tunnel connection is lost. This prevents clients from remaining seemingly connected to the WLAN but without Internet connectivity.

7 Click **Update Settings** to save your changes.

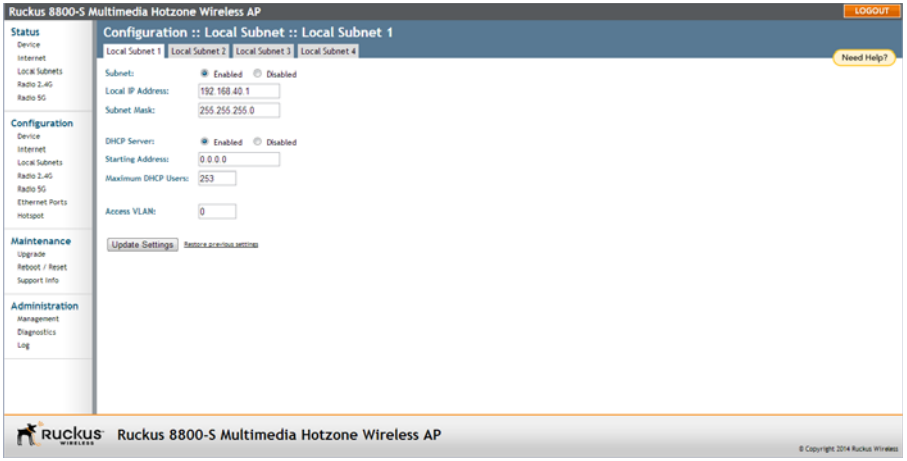
Configuring Local Subnets

ZoneFlex Access Points can be configured to provide routing/network address translation (NAT) functionality using the Local Subnets feature. When a Local Subnet is enabled, the standalone AP serves as a gateway router that can manage its own subnets, providing DHCP server and DNS cache functions for both wired and wireless clients. These clients can be assigned private IP addresses from a user-defined address pool. Traffic from the client station in private address space appears on the outside as if generated by the AP itself. In this way, the AP performs Layer 3 packet forwarding not only for Hotspot/WISPr usage, but for standard usage as well.

Up to four IP subnets can be configured per AP, each with its own VLAN and address range which cannot conflict with one another.

1 Go to **Configuration > Local Subnets**. The *Local Subnet 1* through *Local Subnet 4* tabs allow you to configure each of the four subnets independently.

Figure 32. Configuring local subnets and enabling router mode



2 Click **Enabled** next to *Subnet*. The local subnet configuration options appear.

3 In *Local IP Address,* enter an IP address for the gateway. The default address for Subnet 1 is `192.168.40.1`. This address can be used to access the AP's Web interface for configuration and monitoring from devices connected to this subnet.

4 In *Subnet Mask,* typically you would want to leave the setting at its default value (`255.255.255.0`) for a Class C subnet with an address pool of up to 254 addresses. An error appears if you enter an invalid IP/netmask combination.

5 In *DHCP Server,* click **Enabled** if you want to enable DHCP for this subnet. Starting Address and Maximum DHCP Users fields appear.

6 In *Starting Address,* enter an address in the same subnet as the Local IP Address (for example, **`192.168.40.2`**).

7 In *Maximum DHCP Users,* enter the maximum number of clients that can be assigned addresses by DHCP in this subnet (valid values are 1-253 if the default subnet mask is used).

8 In *Access VLAN,* enter a VLAN ID to segment client traffic arriving from this subnet from other network traffic. (*Example:* If you use the default `192.168.40.1` address range, you would generally use "40" as the VLAN for this subnet.)

9 Click **Update Settings** to save your changes. The local subnet is created immediately and can now be applied to WLANs or Ethernet ports from their respective configuration pages.

Configuring Wireless Settings

This section describes how to configure the wireless settings of the Access Point. There are two types of wireless settings that you need to configure:

- Configuring Common Wireless Settings: Includes the wireless mode, country code, and advanced wireless settings, such as the wireless transmit power and wireless protection mode. These settings are applied to all WLANs.
- Configuring Wireless # Settings: The Wireless # tabs (*Wireless 1* through *Wireless 8* on the 2.4GHz radio and *Wireless 9* through *Wireless 16* on the 5GHz radio) provide settings for customizing each WLAN individually.

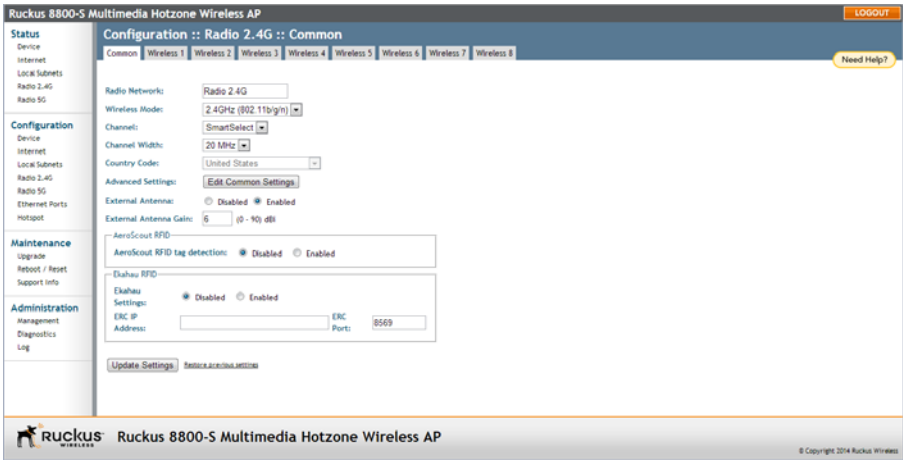
Refer to the sections below for instructions on how to configure each set of wireless settings.

Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. On single-radio APs, go to **Configuration > Wireless**. On dual-radio APs, you configure these settings for the 2.4GHz and 5GHz radios independently by going to **Configuration > Radio 2.4G** or **Configuration > Radio 5G**.

1 Go to **Configuration** > **Wireless/Radio 2.4G/Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

Figure 33. The Configuration > Wireless > Common page



2 Make changes to the common wireless settings listed in the table below.

Table 24. Common Wireless Settings

Setting	Description
Radio Network	(Dual-radio APs only) Allows you to change the name of the 2.4GHz and 5GHz radios (default: *Radio 2.4G* and *Radio 5G*).
Wireless Mode	**On 802.11b/g APs:** The wireless mode options include the following: • *Auto-Select*: Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • *2.4GHz 54Mbps (For faster 802.11g devices only)*: Allows only 802.11g-compliant devices to join the network. • *2.4GHz 11Mbps (For slower 802.11b devices only)*: Allows only 802.11b-compliant devices to join the network. **On dual-radio 802.11n APs:** On dual radio 802.11n APs, the wireless mode is determined by radio; that is, for the 2.4GHz radio, the mode is set to 2.4GHz (802.11b/g/n), while for the 5GHz radio, the mode is set to 5GHz (802.11a/n).
Channel	This option lets you select the channel used by the network. You can choose **SmartSelect**, or choose a specific channel. If you choose *SmartSelect,* then the AP automatically selects the best channel (encountering the least interference) to transmit the signal.
Channel Width (11n APs only)	On 802.11n Access Points, the option to choose 40 MHz channel width theoretically provides double the data capacity of a 20 MHz channel. However, wider channel width means fewer channels available, and more interference with other wireless signals.
Country Code	This option (if enabled) lets you select your country or region code. **CAUTION:** *Selecting the incorrect country or region may result in violation of applicable laws. If you purchased the Access Point in the United States of America, you do not need to set the country code manually. Ruckus Wireless devices that are sold in the USA are preconfigured with the correct country code and this setting is non-configurable.*
Advanced Settings	Refer to "Reviewing Common Advanced Settings" on page 83.

Table 24. Common Wireless Settings (Continued)

External Antenna	**NOTE:** *This option only appears if you are using a ZoneFlex AP with external antenna ports.* Some ZoneFlex APs provide external antenna port(s), in case you want to attach external antenna(s) to extend the range of your wireless network. To enable the AP to use the external antenna(s), select the **Enabled** option in this section. This option is disabled by default.
External Antenna Gain	**NOTE:** *This option only appears if you are using a ZoneFlex AP with external antenna ports and no internal antennas, such as the 7782-E AP.* These ZoneFlex APs require that you correctly set the number of antennas attached to the external antenna ports for each 2.4GHz and 5GHz band. For each band, select **2-Antennas** or **3-Antennas**, as required.
AeroScout RFID	Select **Enabled** to enable AeroScout RFID tag detection.
Ekahau RFID	• Select **Enabled** to enable Ekahau RFID tag detection. • Enter the Ekahau ERC IP address. • Enter the Ekahau ERC port.

3 If you are using AeroScout RFID Tags in your organization to locate assets or personnel, then you can use your ZoneFlex AP to relay location or presence data from the AeroScout Tags to the AeroScout Engine via Wi-Fi.

To enable the AP to relay AeroScout data, click **Enabled** in *AeroScoutRFID tag detection.*

To check the status of the AeroScout communication agent (which relays location data from AeroScout Tags to the AeroScout Engine), go to the **Status > Wireless** page. Refer to "Viewing Current Wireless Settings" on page 117 for more information.

NOTE For other AeroScout-related configuration, refer to the AeroScout documentation that was shipped with your AeroScout Tag and AeroScout Engine.

NOTE If ZoneDirector exists on the network, you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for note-text-bullet

4 If you are using an Ekahau Real Time Location System (RTLS) in your organization, then you can use your ZoneFlex AP to relay location or presence data to the Ekahau Real Time Location System RTLS Controller (ERC).

- To enable the AP to relay Ekahau data, click **Enabled** in *Ekahau Settings.*
- If you have enabled Ekahau, then complete the following:
  - ERC IP Address: Enter an IP address for the Ekahau Real Time Location System RTLS Controller.
  - *ERC port*: 65538 is the default, but it can be set to any available TCP port used by the Ekahau Real Time Location System RTLS Controller.

NOTE For other Ekahau-related configuration, refer to the Ekahau documentation that was shipped with your Ekahau Real Time Location System RTLS Controller.

5 Click **Update Settings** to save your changes.

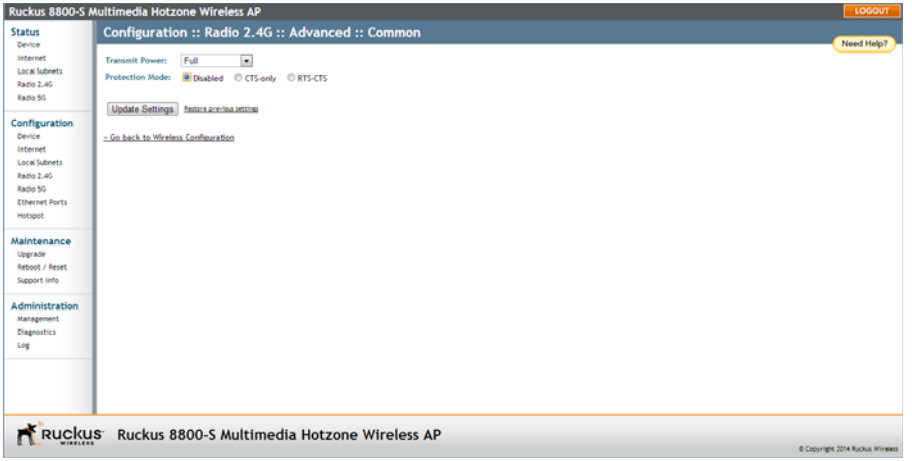
Reviewing Common Advanced Settings

Advanced wireless settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.

NOTE To fully benefit from the Access Point's capabilities, it is advisable not to change these values unless absolutely necessary.

1 On the *Configuration > Wireless/Radio 2.4G/Radio 5G* page, click **Edit Common Settings**. The *Configuration > Wireless > Advanced > Common* page appears.

Figure 34. The Configuration > Wireless > Advanced > Common page



2 Configure the advanced settings listed in Table 25 as required.

Table 25. Advanced wireless common settings

Option	Description
Transmit Power	The default setting is **Full**. Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the predefined power (this value differs according to the current country code).
5.8 GHz Channels	(Only available in certain countries selected using the *Country Code* option.) Select **Enable** to activate the optional 5.8GHz channels (disabled by default).

Table 25. Advanced wireless common settings (Continued)

Protection Mode	(Disabled by default.) When you activate protection, you control how 802.11 devices know when they should communicate with another device. This is important in a mixed environment of both 802.11b and 802.11g/11n clients. **WARNING:** *Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g/11n devices but severely decreases performance.* • **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification. • **RTS-CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.

3 Click **Update Settings** to save and apply the changes.

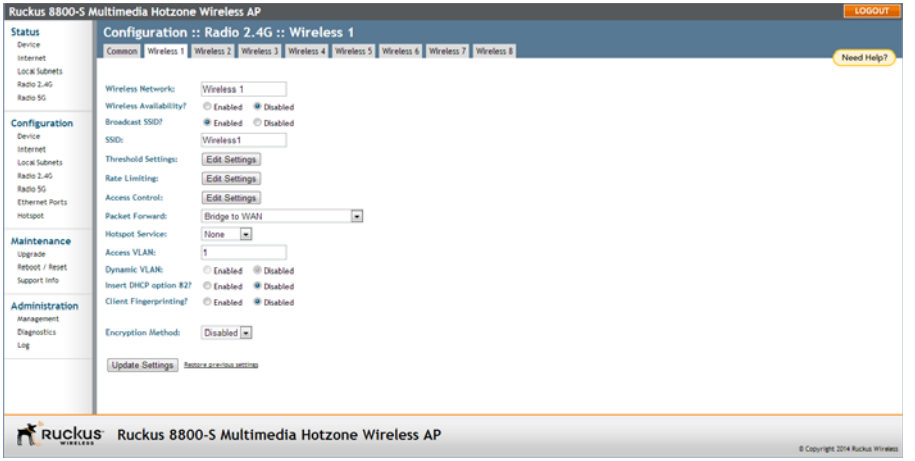
Configuring Wireless # Settings

The Access Point provides up to eight wireless LANs per radio that can be individually configured to provide different kinds of services for different wireless clients, traffic types, or user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.

1 Go to **Configuration** > **Wireless/Radio 2.4G/Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click one of the eight **Wireless (#)** tabs. The *Configuration* > *Wireless* > *Wireless [#]* page appears.

Figure 35. Wireless # settings



3 Review the WLAN options listed in Table 26, and then make changes as required.

Table 26. WLAN options

Option	Description
Wireless Network	This wireless network name is only used for management, and is not visible to wireless clients.
Wireless Availability	This option controls whether or not the wireless network is available to users (**Enabled** or **Disabled**).
Broadcast SSID	This option controls whether or not (**Enabled** or **Disabled**) the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user to use the correct SSID before they can connect to your network.
SSID	This is the publicly-broadcast name of your wireless network. SSIDs can contain up to 32 alphanumeric characters and are case-sensitive. The maximum SSID length can only contain between 2 and 32 characters, including characters from ! (char 33) to ~ (char 126).
Threshold Settings	This button opens a page where you can configure the Protection Mode you activated on the *Configuration* > *Wireless* > *Advanced* > *Wireless [#]* page. If Protection Mode is not active, ignore this option. For more information, see "Setting Threshold Options" on page 95.

Table 26. WLAN options (Continued)

Rate Limiting	This button opens a page where you can configure upload and download limits per station. For more information, see "Rate Limiting" on page 97.
Access Control	This button opens a page where you can configure access controls for the WLAN. For more information, see "Controlling Access to the Wireless Network" on page 97.
Packet Forward	**Isolated**: Selecting *Isolated* causes the traffic from this WLAN to terminate at the Access Point. **Bridge to WAN**: The default setting, *Bridge to WAN* forwards packets arriving on this WLAN to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of wireless packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
Hotspot Service	Select a Hotspot configuration from the list to enable Hotspot service on this WLAN, after you have configured it from the *Configuration > Hotspot* page. Refer to "Configuring Hotspot Service" on page 106.
Local Subnet	This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forwarding*, and allows you to choose which subnet this WLAN's traffic is part of. You must have previously configured a subnet from the *Configuration > Local Subnets* page before it becomes available here.
Access VLAN	Enter a VLAN ID to segment all traffic arriving from this WLAN to a specified VLAN. Default is 1.
Dynamic VLAN	This setting is available only with WPA encryption and 802.1X authentication. Dynamic VLAN allows the dynamic assignment of VLANs to clients based on RADIUS attributes. Enable this option only if your RADIUS server is configured to segment clients using dynamic VLAN.

Table 26. WLAN options (Continued)

Insert DHCP Option 82	When this option is enabled on an SSID, additional information is encapsulated in DHCP option 82 and inserted into DHCP request packets. Current format of option 82 is:
	`Circuit ID sub-option:`
	`WLAN:<IFNAME>:<VLAN>:<SSID>:<MODEL>:`
	`<HOSTNAME>:<DEVMAC>`
	This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

Client Fingerprinting	When this option is enabled the AP attempts to identify client devices by their operating system, device type and host name, if available.
Encryption Method	By default, all data exchanges on your wireless network are not encrypted, but you can select an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings. **CAUTION:** *Ruckus Wireless strongly recommends using WPA as the encryption method as WEP has been proven to be easily circumvented. For more information, see either* "Using WEP" on page 88 *or* "Using WPA" on page 90.

4 When you are finished, click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.

Using WEP

Wired Equivalent Privacy (WEP) is a security algorithm for 802.11 wireless networks designed to provide data confidentiality comparable to that of a wired network. WEP uses a pre-shared key for encrypting data frames that is shared among all users of the wireless network. For this reason and others, WEP has been discredited as a security mechanism and should be avoided in favor of WPA if at all possible.

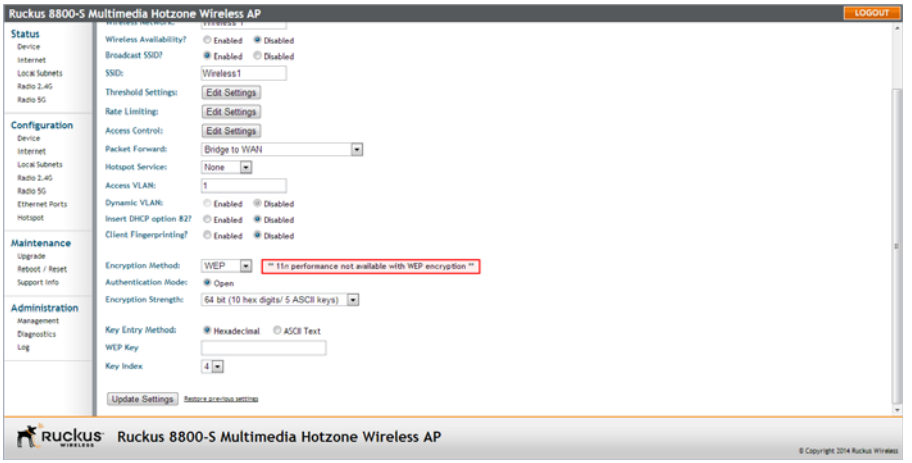
NOTE WEP encryption has been proven to be easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.

NOTE Using WEP encryption limits the performance of this WLAN to 802.11g rates, and other WLANs are unaffected. If you select WEP encryption for a WLAN, wireless devices that are capable of faster 802.11n transfer rates are limited to 802.11g rates.

1 Go to **Configuration** > **Wireless/Radio 2.4G/Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click the **Wireless #** tab that you want to configure. The *Configuration* > *Wireless* > *Wireless[#]* page appears.

Figure 36. WEP settings



3 In the *Encryption Method* menu, select **WEP**. An additional set of WEP-specific encryption options appear.

4 Review the encryption settings listed in Table 27, and then make changes as required.

Table 27. WEP Options

Encryption Setting	Description
Authentication Mode	*Open* is the only authentication mode available with WEP encryption.

Table 27. WEP Options (Continued)

Encryption Strength	• **64 bit**: Specify the key with 10 hexadecimal digits or 5 ASCII characters. • **128 bit**: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.
Key Entry Method	• **Hexadecimal**: The encryption key only accepts hexadecimal characters (0-9, A-F). • **ASCII Text**: The encryption key accepts ASCII characters.
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from “1” to “4”, that the WEP key is to be stored in.

5 Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

Using WPA

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols developed by the Wi-Fi Alliance in response to the weaknesses of WEP.

Selecting WPA as the Encryption Method allows you to choose WPA version, WPA Authentication and WPA Algorithm. This section discusses WPA-PSK (pre-shared key). For information on WPA-Enterprise (WPA-802.1X), see “Customizing 802.1X Settings” on page 93.

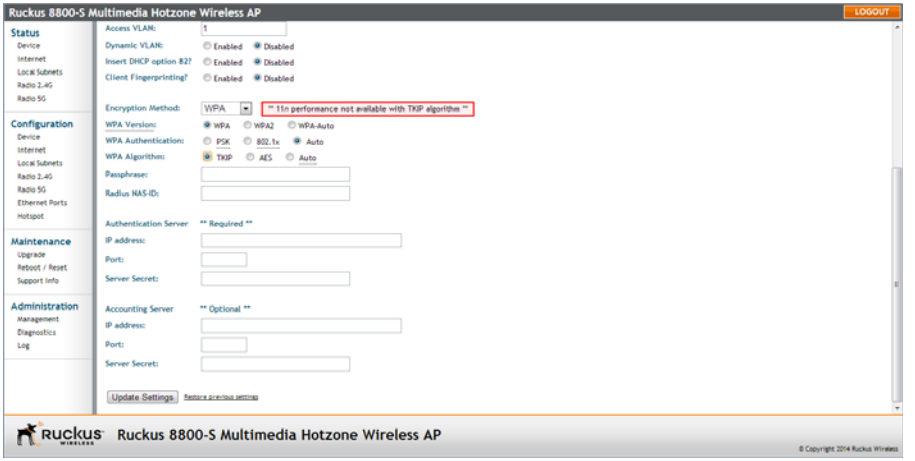
WPA-PSK (also known as WPA-Personal) allows automatic key generation based on a single passphrase. WPA-PSK provides strong security for small and medium organizations and does not require a RADIUS server, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the WLAN with WPA-PSK, wireless users are not able to connect to your WLAN unless their devices support WPA-PSK and are configured with the same passphrase.

1 Go to **Configuration** > **Wireless/Radio 2.4/Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click the **Wireless #** tab that you want to configure. The *Configuration* > *Wireless* > *Wireless [#]* page appears.

Figure 37. WPA settings



3 Click the **Encryption Method** menu, and select **WPA**. An additional set of WPA-specific options appear.

4 Review the encryption settings listed in Table 28, and then make changes as required.

Table 28. Encryption settings

Encryption Setting	Description
WPA Version	Your options are *WPA, WPA2* or *WPA Auto.* • **WPA** (Wi-Fi Protected Access) is the replacement security standard adopted by the Wi-Fi Alliance in response to the security weaknesses of WEP. WPA was developed as an interim measure before ratification of the 802.11i standard, which introduced WPA2. • **WPA2** provides stronger wireless security than WPA and is the recommended option. However, older wireless clients may not be compatible with WPA2. For example, WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later. • **WPA-Auto** allows both WPA and WPA2 devices to operate on the same WLAN.
WPA Authentication	• **PSK** (Pre-Shared Key) mode is suitable for home or personal use. • **802.1x** mode uses a RADIUS server to verify user identity. • **Auto** mode offers both options to the wireless client. For more information on how to configure the 802.1X mode, refer to "Customizing 802.1X Settings" on page 93.
WPA Algorithm	• **TKIP**: Temporal Key Integrity Protocol is an older encryption algorithm that provides stronger security than a shared WEP key, but not as strong as the newer AES algorithm. • **AES**: AES (Advanced Encryption Standard) replaces TKIP as the default (and recommended) encryption algorithm for modern wireless LANs. • **Auto**: Auto allows both encryption algorithms to be used on the same WLAN. When Auto is selected, the wireless client decides whether TKIP or AES is used. Note however that allowing TKIP reduces the performance of the WLAN (as broadcast packets are limited to slower transfer rates), and is therefore not recommended.
Passphrase	Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).

5 Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

Customizing 802.1X Settings

NOTE Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

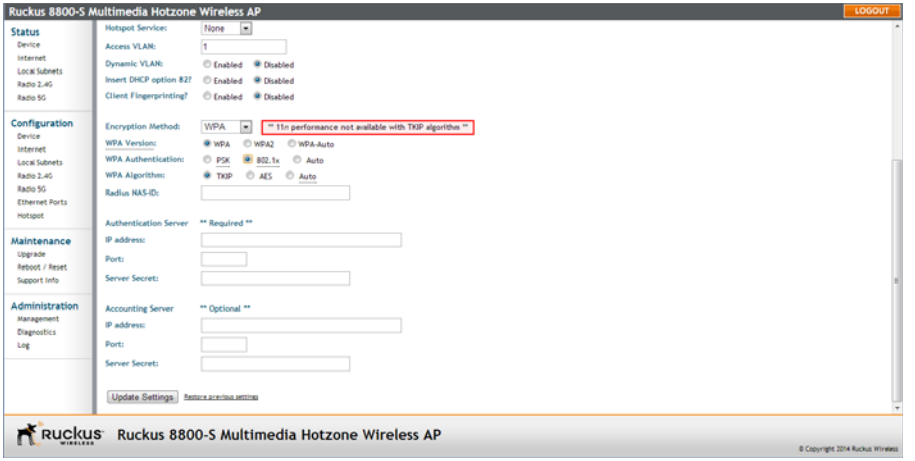
If you choose *WPA* as the encryption method, then you have the option to set up the Access Point to act as an 802.1X proxy, using external authentication sources such as a RADIUS server.

In 802.1X authentication, the supplicant sends access request messages along with credentials, such as user name/password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification. The supplicant (client device) remains in an unauthorized state until verification has been received. In unauthorized state, only 802.1X traffic is allowed; all other traffic, such as DHCP and HTTP traffic, is dropped. For its wireless interfaces, the Access Point can serve as the authenticator communicating between the supplicant and the authentication server.

1 Go to **Configuration** > **Wireless/Radio 2.4G/Radio 5G**. The *Configuration > Wireless > Common* page appears.

2 Click a **Wireless #** tab to configure. The *Configuration > Wireless > Wireless [#]* page appears.

Figure 38. 802.1X settings



3 In the *Encryption Method* menu, select **WPA**. The basic set of WPA-specific encryption options appears on the page.

4 In *WPA Authentication* select the required WPA authentication type:

- **WPA** (Wi-Fi Protected Access) is the replacement security standard adopted by the Wi-Fi Alliance in response to the security weaknesses of WEP. WPA was developed as an interim measure before ratification of the 802.11i standard, which introduced WPA2.
- **WPA2** provides stronger wireless security than WPA and is the recommended option. However, older wireless clients may not be compatible with WPA2. For example, WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later.
- **WPA-Auto** allows both WPA and WPA2 devices to operate on the same WLAN.

5 Select **802.1x** as the *WPA Authentication* mode. Additional options appear.

6 In *WPA Algorithm* select one of the following:

- **TKIP**: Temporal Key Integrity Protocol is an older encryption algorithm that provides stronger security than a shared WEP key, but not as strong as the newer AES algorithm.
- **AES**: AES (Advanced Encryption Standard) replaces TKIP as the default (and recommended) encryption algorithm for modern wireless LANs.

- **Auto**: Auto allows both encryption algorithms to be used on the same WLAN. When Auto is selected, the wireless client decides whether TKIP or AES is used. Note however that allowing TKIP reduces the performance of the WLAN (as broadcast packets are limited to slower transfer rates), and is therefore not recommended.

7 Configure the following settings to customize your 802.1X authentication:

- *Radius NAS-ID:* Enter the Network ID assigned to your Access Point in the RADIUS server Client list.
- *Authentication Server (required):* Enter the information needed to establish a connection between the Access Point and the RADIUS server.
- *Accounting Server (optional):* Enter the information needed to establish this connection.

8 Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.

NOTE Ruckus Wireless APs do not support arbitrary rate values for 802.1X clients (if client rate limiting attributes are configured on the RADIUS server). ZoneFlex APs support only those WLAN rate limiting values that can be set using the AP web interface. If the rate returned by the RADIUS server does not match one of these values exactly, it is approximated.

Setting Threshold Options

The following options allow you to fine-tune the *Protection Mode* behavior, set previously on the *Configuration* > *Wireless* > *Advanced* > *Common* page. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, which determine what is put into effect and when.

NOTE Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

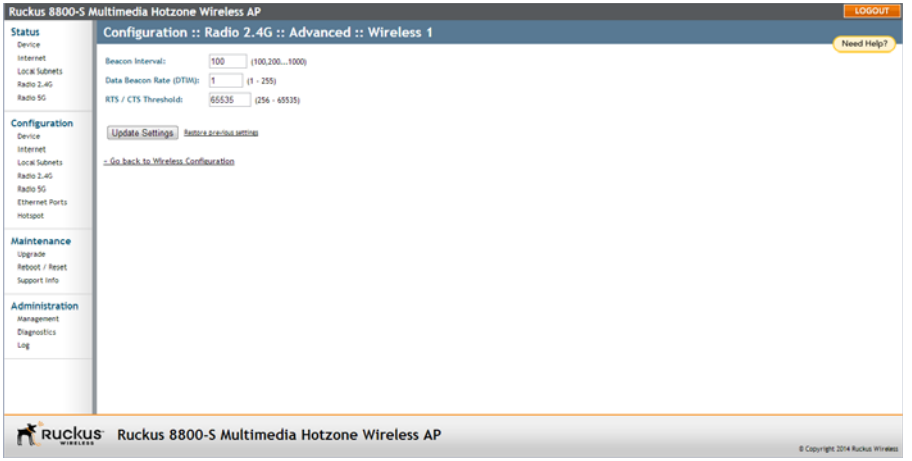
---

1 Go to **Configuration > Wireless/Radio 2.4G/Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click the tab for the **Wireless #** (WLAN) that you want to configure. The *Configuration* > *Wireless* > *Wireless [#]* page appears.

3 Look for *Threshold Settings,* and then click **Edit Settings**. The *Configuration* > *Wireless* > *Advanced* > *Wireless [#]* page appears.

Figure 39. Threshold settings



4 Review the options listed in Table 29, and then make any needed changes.

Table 29. Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in milliseconds. A beacon is a broadcast packet sent by the AP to synchronize the wireless network.
Data Beacon Rate (DTIM)	(The default value is 1.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.
RTS/CTS Threshold	(The default value is 65535.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in an environment with excessive signal noise or hidden nodes, but may result in some performance degradation.

5 Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

You have completed configuring the threshold options. To reopen the previous page, click the **Go back to Wireless Configuration** link.

Rate Limiting

Rate Limiting allows you to cap per-client data transfer rates for a specific WLAN.

1 Go to **Configuration > Wireless/Radio 2.4G/Radio 5G**.

2 Select the WLAN that you want to configure from the tabs at the top of the page.

3 Click the **Edit Settings** button next to *Rate Limiting*. The *Rate Limiting* page appears.

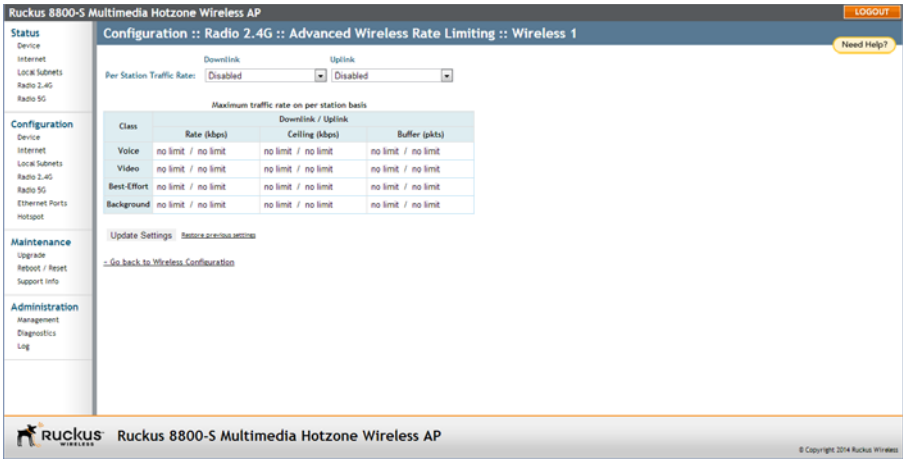
4 Set the maximum *Downlink* and *Uplink* rate per station.

The table below your selections updates to show the maximum transfer rate per station for each traffic type.

5 Click **Update Settings** to save your changes.

You have completed configuring the rate limiting options. To reopen the previous page, click the **Go back to Wireless Configuration** link.

Figure 40. Limit per station traffic rates on a specific WLAN



Controlling Access to the Wireless Network

Access Control enables you to specify the stations are allowed to join (associate with) your wireless networks. Access controls can be configured for each WLAN from its respective *Wireless #* tab.

Access Control List (ACL) Options

This section describes the options that you can use to control access to the wireless network.

- **Disable WLAN access restrictions:** The MAC-address-based restrictions on which stations can join the WLAN are disabled, so any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption passphrase. When this option is selected, the *Access Controls* table is hidden.
- **Allow only stations listed in the Access Control Table:** Only stations entered into the access-controls table are allowed, but all others are disallowed. To add MAC addresses, see "Changing Access Controls for a WLAN" on page 98.
- **Deny only stations listed in the Access Control Table:** Stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see "Changing Access Controls for a WLAN" on page 98.

Changing Access Controls for a WLAN

By default, the **Disable WLAN access restrictions** option is selected, which allows any wireless station to gain access to the wireless network. If you want to change this setting, follow the instructions below.

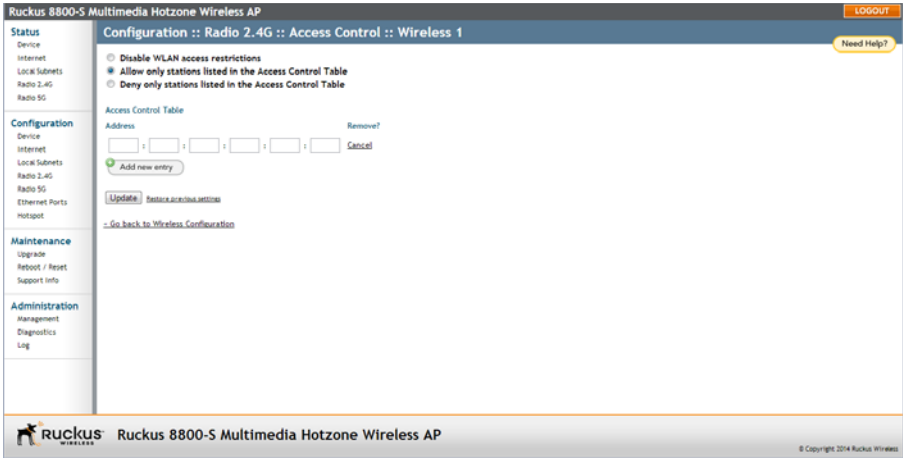
1 Go to **Configuration** > **Wireless/Radio 2.4G/Radio 5G**.

2 Click the **Wireless #** tab for which you want to configure the access control settings.

3 Click the **Edit Settings** button next to *Access Control*.

4 Select the radio button for the desired access control. (For a description of the options, refer to "Access Control List (ACL) Options".) The *Access Controls Table* appears.

Figure 41. Access control settings



5 To add a MAC address to the Access Control table, click the **Add new entry** button.

6 Fill out the **Address** text boxes: Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. Allowable hex-digit characters are 0-9, a-f, and A-F.

7 Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row is added to the table. You have completed adding an entry to the MAC address table.

8 If you have additional MAC addresses you want included, then click **Add new entry**, and then repeat these steps until you have entered all the stations you want. There is a limit of 128 rows.

Removing a MAC Address

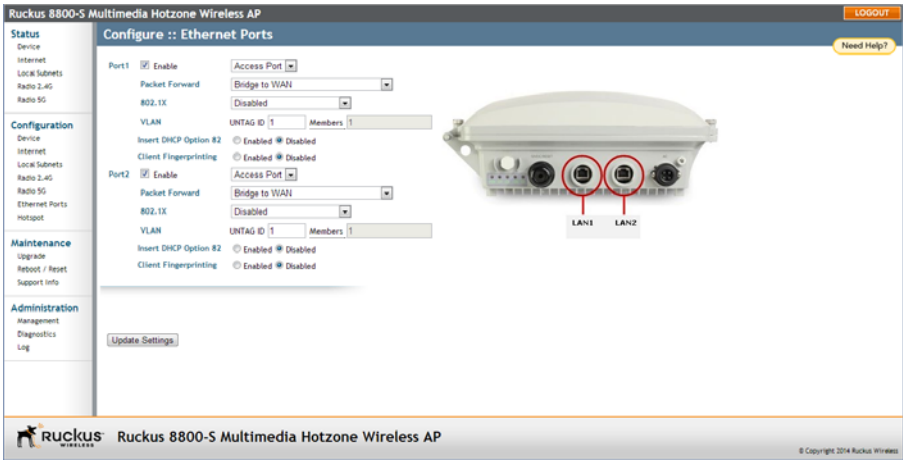
To remove a MAC address from the ACL table, click the **Cancel** button in the *Remove* column, and then click **Update**. The ACL table refreshes, and the MAC address that you deleted disappears from the table.

Configuring Ethernet Ports

The Ethernet Ports configuration page allows you to define how the Access Point's Ethernet ports behave. You can disable ports entirely, define trunking and packet forwarding behavior, configure 802.1X authentication settings, and individually configure VLAN settings for each port from this page.

1 Go to **Configuration > Ethernet Ports**.

Figure 42. The Configuration > Ethernet Ports page



2 Review the following table and make changes as needed for each of the ports labeled **PORT 1** through **PORT 4** (depending on AP model), which correspond to the AP's Ethernet ports.

Table 30. Individual Ethernet port options

Setting	Description
Enable	All Ethernet ports are enabled by default. Unchecking this box next to a port disables that port entirely. If you do not want to provide wired access through the AP, uncheck (clear) the **Enable** box next to each LAN port.
Port Type	See "Setting Ethernet Port Type" on page 103 for more detailed information. • **Trunk Port**: This port passes all VLAN traffic. • **Access Port**: This port provides network access. • **General Port**: User-defined VLAN membership.

Table 30. Individual Ethernet port options (Continued)

Packet Forward	**Isolated**: Selecting *Isolated* causes the traffic from this port to terminate at the Access Point. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
802.1X	Configure the port as an 802.1X authenticator or supplicant. The following options are available: • **Disabled**: No 802.1X controls are applied to this port. • **Authenticator (Port-Based)**: Only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. • **Authenticator (MAC-Based)**: Each MAC host is individually authenticated. • **Supplicant:** The port acts as a supplicant to an upstream authenticator. Configure a port as Supplicant if the port is a Trunk Port used to connect the AP to a LAN switch. See "Working with 802.1X on Wired Ethernet Ports" on page 104 for more information.
	Enable MAC authentication bypass: Mark to enable or clear to disable. Only available if 802.1X is enabled.
Local Subnet	This option appears if you have selected *Local Subnet and Route to WAN* under *Packet Forwarding*, and you have selected *Access Port* as the port type. This option allows you to select which subnet this port's traffic is part of. You must have previously configured a subnet from the *Configuration* > *Local Subnets* page before it becomes available here.

Table 30. Individual Ethernet port options (Continued)

VLAN	• **UNTAG ID**: Enter a valid VLAN ID in this field to segment traffic arriving on this port to a specific VLAN. Default is 1. Valid VLAN entries are 1-4094. • **Members**: Displays the VLAN membership of the port. (Membership is configurable only for the *General* port type.) • **Guest VLAN**: Enter the guest VLAN, from 1 to 4094. • **Enable Dynamic VLAN**: Enable dynamic VLAN only with 802.1X authentication. Dynamic VLAN allows the dynamic assignment of VLANs to clients based on RADIUS attributes. Enable this option only if your RADIUS server is configured to segment clients using dynamic VLAN. Refer to "Working with Port-Based VLANs" on page 104 for more information.

Insert DHCP Option 82	When this option is enabled for an Ethernet port, additional information is encapsulated in DHCP option 82 and inserted into DHCP request packets.
	The current format of option 82 is:
	`Circuit ID sub-option:`
	`ETH:<IFNAME>:<VLAN>:N/A:`
	`<MODEL>:<HOSTNAME>:<DEVMAC>`
	This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

Client Fingerprinting	When this option is enabled the AP attempts to identify client devices by their operating system, device type and host name, if available.

3 Review the following table and make changes as needed for all of the Ethernet ports.

Table 31. All Ethernet port options

Setting	Description
Authentication Server (required)	Enter the authentication server IP address, port, and server secret for all Ethernet ports. Only available if 802.1X Authenticator are enabled (includes any packet forward selection).

Table 31. All Ethernet port options (Continued)

Accounting Server (optional)	Enter the accounting server IP address, port, and server secret for all Ethernet ports. Only available if 802.1X Authenticator are enabled (includes any packet forward selection).
Supplicant User Name and Supplicant Password	Enter the 802.1X supplicant user name and password for all Ethernet ports. Only available if 802.1X Trunk port and Supplicant are enabled (includes any packet forward selection).

4 Click **Update Settings** to save your changes.

Setting Ethernet Port Type

ZoneFlex AP Ethernet ports can be configured as one of the following port types:

- Trunk Port
- Access Port
- General Port

Trunk Port

Trunk Ports forward and receive tagged and untagged frames and are used for bridging switch ports together. The Trunk port is a member of all VLANs that exist on the switch, and all VLAN-tagged traffic arriving on the port is seen. If an untagged frame is received on a Trunk port, the frame is associated with the Untag VLAN (also known as the *native VLAN*, by default, 1).

If a port is configured as a Trunk port, the Untag ID field can be used to define the Untag VLAN--the VLAN that the switch uses for forwarding and filtering when a frame arrives without an 802.1Q header.

Access Port

Access Ports are used to provide network access. Traffic arriving on different Access Ports can be segmented into different logical networks (VLANs) using the Untag VLAN ID field. Access Ports are members of only one VLAN--the VLAN that is configured in the Untag VLAN field.

General Port

The General Port can be configured to support multiple tagged VLANs and one untagged VLAN. As Trunk Ports by definition are members of all VLANs, the General Port is the only port type for which membership is user configurable for multiple VLANs.

Working with Port-Based VLANs

The Access Point provides options for segmenting all incoming traffic (both wireless and wired Ethernet traffic) into specific VLANs. There are two ways to segment incoming traffic into VLANs:

- Each of the wireless interfaces (SSIDs) can be configured with a specific Access VLAN ID: (**Configuration > Wireless > Wireless [#] > Access VLAN**).
- Each of the LAN ports can be configured with an Untag VLAN ID (**Configuration > Ethernet Ports > VLAN > Untag ID**).

For Ethernet ports, the behavior of the Untag VLAN ID depends on the Port Type selected. If the port is configured as a Trunk port, it includes all VLANs (1-4094) in its membership. The VLAN Untag ID field (default = 1) can be used to redefine the *Native VLAN* for the port.

If the Ethernet port is configured as an Access Port, it can be configured with only one Untag VLAN ID and its membership includes only that one VLAN.

If the Ethernet port is configured as a General Port, it can be configured to include multiple VLANs in its membership and one Untag VLAN.

Working with 802.1X on Wired Ethernet Ports

802.1X authentication consists of the following three components:

- *Supplicant*: The supplicant sends access request messages along with credentials, such as user name/password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification.
- *Authenticator*: The authenticator challenges the identity of the supplicant, then passes its credentials to the AAA server. If the credentials are accepted the supplicant is allowed access.
- *Authentication Server (AAA Server)*: The AAA server verifies the supplicant's credentials and permits or rejects its request for access.

For wired 802.1X, a Ruckus AP's Ethernet port can be configured as either an *Authenticator* or as a *Supplicant*, depending on which port type is selected. Table 32 and Table 33 describe the 802.1X roles available by port type.

Table 32. Authenticator support by port type

	Trunk Port	Access Port	General Port
Port-based mode	X	X	X
MAC-based mode		X	

Table 33. Supplicant support by port type

	Trunk Port	Access Port	General Port
Supplicant	X		

The following considerations apply:

- A single port cannot be configured as both an *Authenticator* and *Supplicant* at the same time.
- Only one port per AP can be configured as a *Supplicant*.
- If the AP is connecting to a switch port with 802.1X authentication enabled, the AP's port type should be configured as a Trunk Port and its role should be configured as *Supplicant*. The switch port should be configured as a Trunk port in *Port-based Authenticator* mode.
- If there are multiple devices connected to an AP port (through a downstream switch), the port can be configured as either *Port-based* or *MAC-based Authenticator*. In Port-based mode, only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. In MAC-based mode, each MAC host is individually authenticated.
- If a Trunk Port is configured as a *Supplicant*, a user name and password must be entered to authenticate the port to the 802.1X-aware LAN switch.
- If an Access Port is configured as an *Authenticator*, the administrator must define the RADIUS server that the Authenticator communicates with. All Ethernet ports of a single AP are configured with the same RADIUS server.

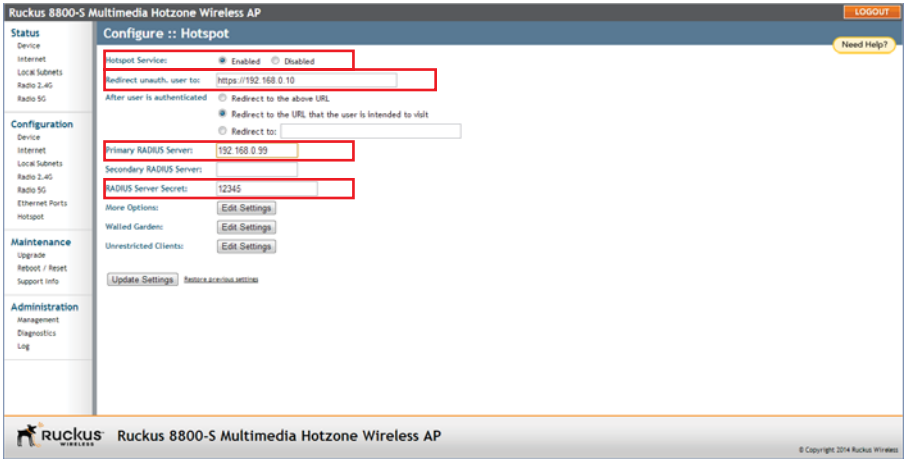
Enable MAC authentication bypass: If MAC authentication bypass is enabled, the port first attempts to authenticate the attached device by MAC address, and if that fails, it tries to authenticate the device using 802.1X.

Configuring Hotspot Service

Hotspot service can be deployed on standalone ZoneFlex APs through the Web interface. At a minimum, you must configure a login redirect URL and a RADIUS server to which users are authenticated. Additional options and controls are provided on subsequent pages.

1 Go to **Configuration > Hotspot**.

Figure 43. Minimum configuration settings for providing Hotspot service



2 Click **Enabled** next to *Hotspot Service*.

3 Review the settings in Table 34, and make changes as needed.

Table 34. Hotspot configuration settings

Setting	Description
Redirect unauth. user to	Redirect unauthenticated users to the specified URL (login page).

Table 34. Hotspot configuration settings (Continued)

Setting	Description
After user is authenticated	Select where you want to redirect the user after successful authentication. • *Redirect to the above URL*: Return to the login URL configured above. • *Redirect to the URL the user intended to visit*: Upon successful authentication, go directly to the URL that the user originally entered (typically the browser's home page). • *Redirect to*: Specify a URL to which users are redirected after authentication. This can be used to redirect users to a "Login Successful" page, or a page that offers connection time information or a Logout button.
Primary RADIUS Server	Enter the IP address of the primary RADIUS server against which users are authenticated (required).
Secondary RADIUS Server	Enter the IP address of the secondary RADIUS server, if one is available (optional).
RADIUS Server Secret	Enter the shared secret for communication with the RADIUS server (required).

4 Click **Update Settings** to save your changes.

You have completed the minimum settings for providing Hotspot service on this AP. Additional configuration options are available using the *Edit Settings* buttons at the bottom of the page.

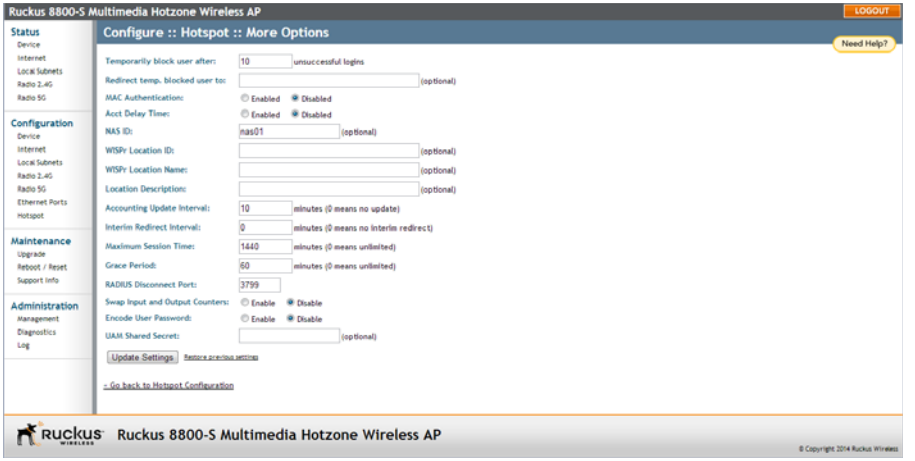
Customizing Hotspot Optional Settings

Optional Hotspot settings include a number of options for fine-tuning your Hotspot service, such as maximum session time, grace period, accounting update interval, and so on.

1 Go to **Configuration > Hotspot**.

2 Click *More Options/***Edit Settings.**

Figure 44. Configuring optional Hotspot options



3 Configure these Hotspot options from the *Configuration* > *Hotspot* > *More Options* page:

Table 35. Optional Hotspot settings

Setting	Description
Temporarily block user after __ unsuccessful logins	Specify the maximum number of repeated authentication failures allowed.
Redirect temp. blocked user to	Enter a redirect URL to which blocked users are redirected.
MAC Authentication	When **Enabled** the Hotspot service attempts to authenticate users based on their MAC addresses if the local Hotspot authentication has failed. If enabled, an optional MAC authentication password can be entered. If no password is specified, the system uses the client's MAC address as the password.

Table 35. Optional Hotspot settings (Continued)

Acct Delay Time	Accounting delay **Enabled** or **Disabled**. This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. When enabled, this attribute appears in accounting request packets with a starting value of “0”, incremented each retry packet. When disabled, this attribute is not included in any accounting request packet.
NAS ID	Specify the Network Access Server identifier of this device. The NAS-ID attribute is sent in RADIUS access and accounting request messages. It can also be used as location identification when NAS-IP-Address cannot be used for this purpose.
WISPr Location ID	Specify the Hotspot location identifier. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of “isocc=<ISO_Country_Code>, cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>”.
WISPr Location Name	Specify the hotspot location and operator's name. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of “<HOTSPOT_OPERATOR_NAME>,<Location>”.
Location Description	Specify the description of location. This value is provided in the HTTP redirection.
Accounting Update Interval	Specify the interval for RADIUS accounting requests.
Interim Redirect Interval	Specify the interval after which users are redirected to the login URL.
Maximum Session Time	Enter the maximum session time in minutes.
Grace Period	Specify the maximum time that a user may disconnect from the Hotspot service and return without the need to login again.

Table 35. Optional Hotspot settings (Continued)

RADIUS Disconnect Port	UDP port to listen to for accepting RADIUS disconnect requests.
Swap Input and Output Counters	Swap the value of input counters (packets, octets and giga words) and output counters in RADIUS accounting requests. This option is mainly for backward compatibility with existing Chillispot deployments.
Encode User Password	Encode user password with challenge string, if UAM secret is not specified; otherwise, encode user password with both challenge string and UAM secret.
UAM Shared Secret	The UAM Shared Secret is the shared secret between this Access Point and the HTTP server for the Redirection URL. This setting is optional.

4 Click **Update Settings** to save your changes.

Creating a Hotspot Walled Garden

You can use the Hotspot Walled Garden rules to designate network destinations (host address or subnet) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden.

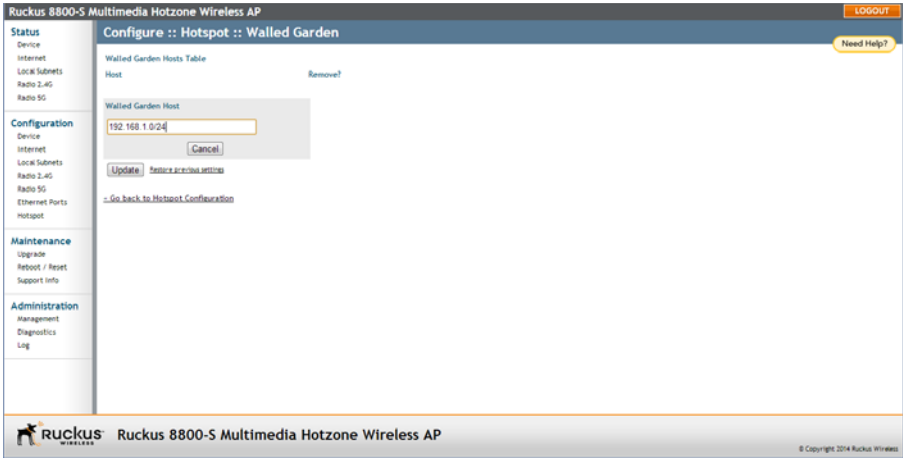
URLs are resolved to an IP address (up to four). Users may not be able to click through to other URLs presented on a page, if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to reauthenticate when they navigate through the page.

1 Go to **Configuration > Hotspot**.

2 Click *Walled Garden/***Edit Settings.**

3 Click **Add new entry**. A field entitled *Walled Garden Host* appears.

Figure 45. The Walled Garden hosts table



4 In *Walled Garden Host*, enter a host name, IP address, network segment (for example, `192.168.1.0/24`) or a domain name. If a domain name is entered, it is resolved every 5 minutes.

5 Click **Update** to save your entry.

You can create up to 64 entries in the Walled Garden Hosts table.

Removing Entries from the Walled Garden Hosts Table

1 Click the check box next to the entry you want to remove, under the *Remove?* column.

2 Click **Update**. The entry is removed from the list.

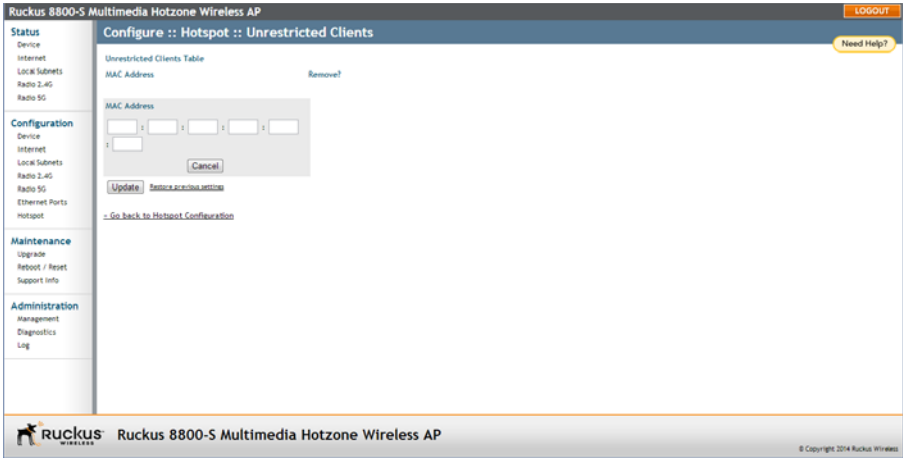
Allowing Unrestricted Hotspot Access by MAC Address

1 Go to **Configuration > Hotspot**.

2 Click *Unrestricted Clients/***Edit Settings.**

3 Click **Add new entry**, and enter the MAC address of a client in the fields provided.

Figure 46. Configuring Hotspot unrestricted clients table



4 Click **Update** to save your changes.

Managing the Access Point

4

In this chapter:

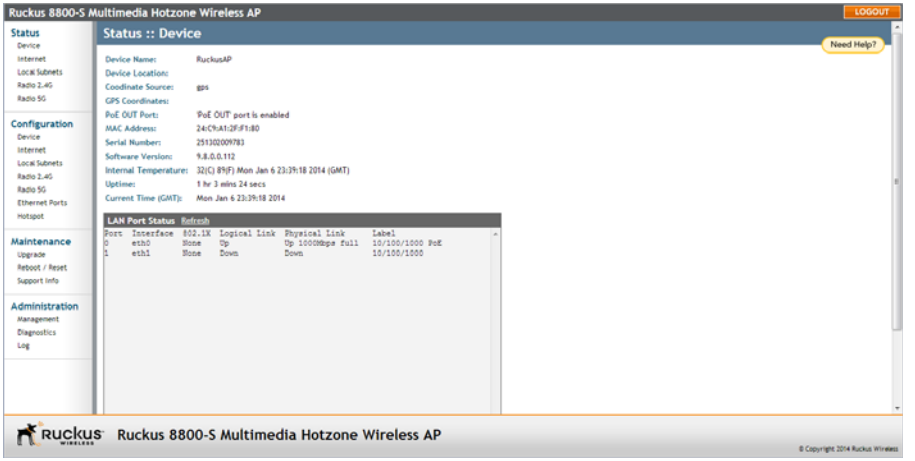
- Viewing Current Device Settings
- Viewing Current Internet Connection Settings
- Viewing Current Local Subnet Settings
- Viewing Current Wireless Settings
- Viewing Associated Wireless Clients
- Viewing Current Wireless Settings
- Viewing Associated Wireless Clients
- Changing the Administrative Login Settings
- Enabling Other Management Access Options
- Working with Event Logs and Syslog Servers
- Upgrading the Firmware
- Rebooting the AP and Cable Modem
- Resetting the AP to Factory Defaults
- Running Diagnostics
- Where to Find More Information

This chapter provides instructions for managing standalone ZoneFlex Access Points using the Web interface. For information on managing your ZoneFlex network using ZoneDirector, refer to the *ZoneDirector User Guide,* available from the Ruckus Wireless website.

Viewing Current Device Settings

The *Status* > *Device* page displays a general overview of the AP's current status, including device name, serial number, MAC address, current software version, and so on.

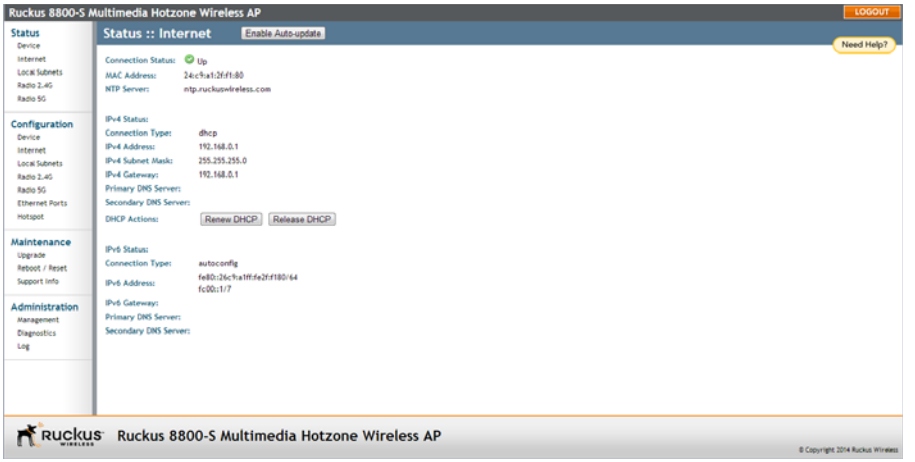
Figure 47. The Status > Device page



Viewing Current Internet Connection Settings

The *Status* > *Internet* page displays information on the AP's network settings; that is, the settings that allow the AP to communicate with your local network and the Internet. Information includes IP address, gateway, DNS server, NTP server and connection type (method of obtaining an IP address -- DHCP or static IP).

Figure 48. The Status > Internet page

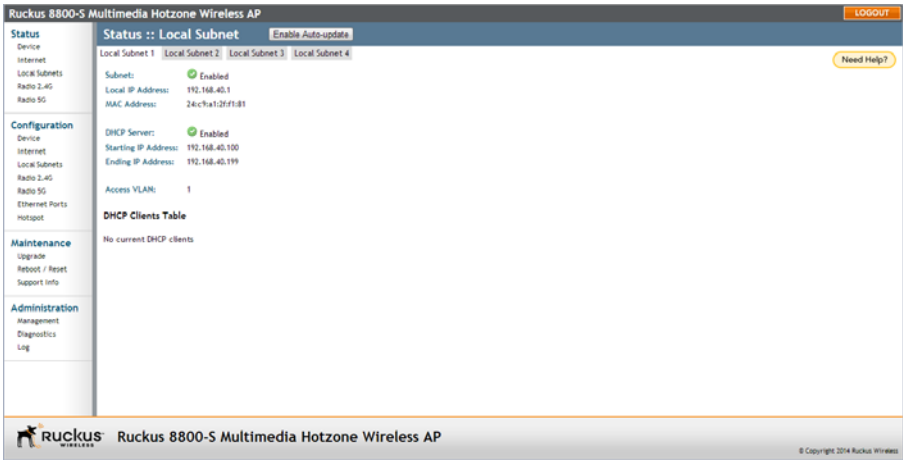


Viewing Current Local Subnet Settings

The *Status* > *Local Subnets* page can be used to view the router (local subnet) configurations and list of any clients connected to those subnets.

If you want to make changes to any of these settings, then go to **Configuration > Local Subnets**. Refer to "Configuring Local Subnets" on page 78 for more information.

Figure 49. The Status > Local Subnet page



Viewing Current Wireless Settings

If you want to view the current common wireless settings that the AP is using, go to the **Status** > **Wireless** page (on dual-band APs, go to **Status > Radio 2.4G** or **Status > Radio 5G**).

Figure 50. The Status > Wireless (Radio 2.4G/5G) page

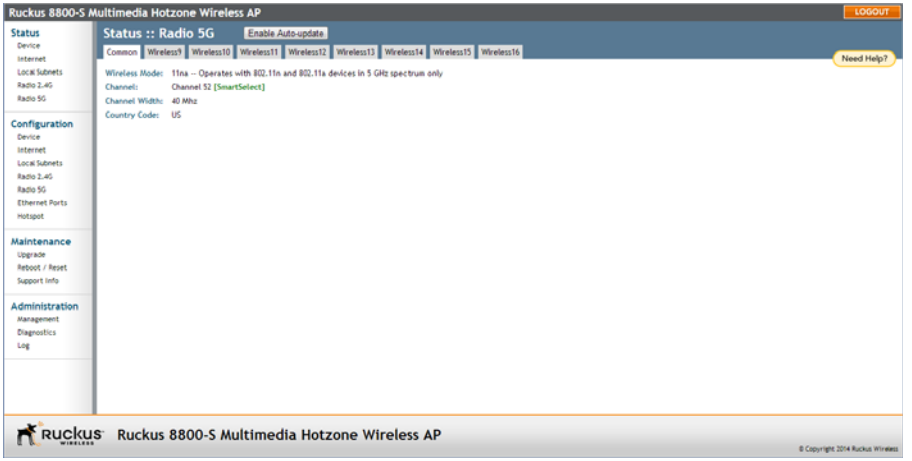


Table 36 lists the descriptions of each wireless setting.

Table 36. Common Wireless settings

Setting	Description
Wireless Mode	Shows the wireless mode that the AP is currently using. Possible values include: • *Auto-Select:* (For 802.11b/g APs only) Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • *2.4GHz 54 Mbps:* Allows 11g devices only. • *2.4GHz 11 Mbps:* Allows 11b devices only. • *11ng:* Operates with 802.11n, 802.11g and 802.11b devices in the 2.4GHz spectrum only. • *11na:* Operates with 802.11n and 802.11a devices in the 5GHz spectrum only.

Table 36. Common Wireless settings (Continued)

Channel	Shows the wireless channel that the AP is currently using. If you set the wireless channel to *SmartSelect,* this field shows the value *Channel # [SmartSelect].*
Channel Width	11n devices only. Displays whether the channel width is set to *20MHz* or *40MHz.*
Country Code	Shows the country code that the AP has been set to use. **CAUTION:** *Verify that the AP is using the correct country code to make sure it uses only the allowed radio channels in your region. Selecting the incorrect country code may result in violation of applicable laws.*
AeroScout RFID tag detection	Shows *Enabled* if you enabled AeroScout RFID tag detection. The default setting is *Disabled.*
AeroScout Engine communication daemon	Shows *Up* if the communication agent on the AP is able to relay location data from AeroScout Tags to the AeroScout Engine. If the communication agent is unable to relay data or AeroScout tag detection is disabled, this field shows *Down.*
Ekahau Engine communication daemon	Shows *Enabled* if you enabled Ekahau RFID tag detection. The default setting is *Disabled.*
ERC IP	Ekahau Real Time Location System RTLS Controller IP address.
ERC Port	TCP port used by the Ekahau Real Time Location System RTLS Controller.

If you want to make changes to any of these settings, go to the **Configuration** > **Wireless/Radio 2.4G/Radio 5G** page. Refer to "Configuring Common Wireless Settings" on page 80 for more information.

Viewing Associated Wireless Clients

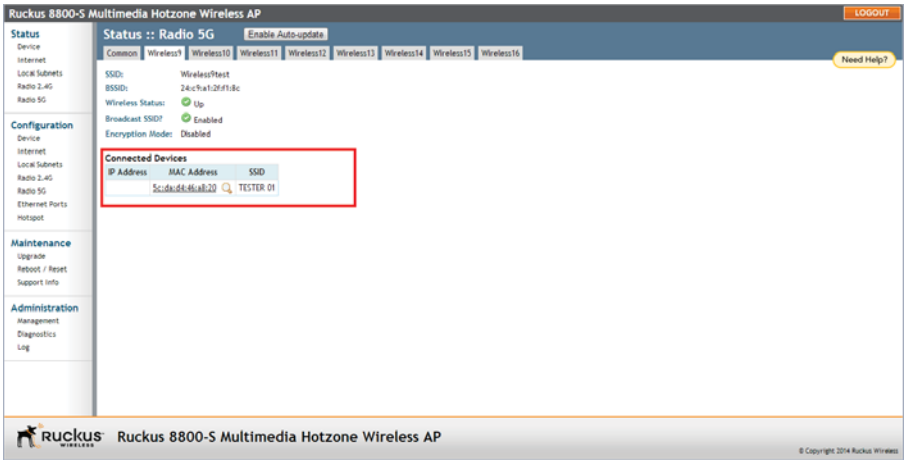
A usage-monitoring capability has been built into the Access Point to help you monitor wireless clients that are associated with your wireless network.

1 Go to **Status** > **Wireless**. The *Status* > *Wireless* page appears.

NOTE If you are using a dual-band ZoneFlex AP, go to **Status > Radio 2.4G** or **Status > Radio 5G**.

2 Click any of the **Wireless #** tabs. Wireless clients that are associated with this particular wireless network appear under *Connected Devices.*

Figure 51. Viewing connected devices



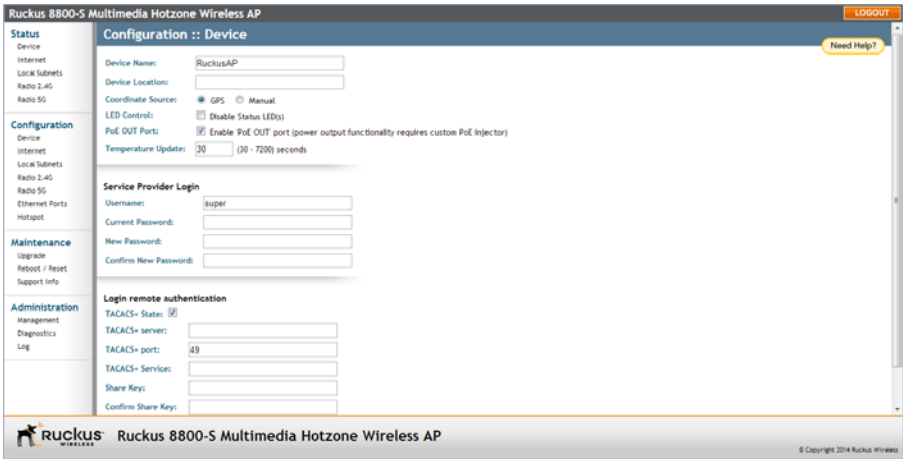
Changing the Administrative Login Settings

The default user name is `super` and the default password is `sp-admin`. To prevent unauthorized users from logging into the Web interface using these default administrator login settings, Ruckus Wireless recommends that you change the default Web interface password immediately after your first login.

1 Log into the Web interface.

2 Go to **Configuration** > **Device**.

Figure 52. The Configuration > Device page



3 Under *Service Provider Login,* change the default administrator login settings:

- In *Username,* type a new user name that you will use to log in to the Web interface. The default user name is `super`.
- When you are changing a password, type the existing password in *Current Password.*
- In *New Password,* type a new password to replace the existing password. The password must consist of six to 32 alphanumeric characters only.
- In *Confirm New Password,* retype the new password.

4 Click **Update Settings**. The message *Your parameters were saved* appears.

You have completed changing the default login settings. The next time you log in to the Web interface, make sure you use these updated login settings.

Enabling Other Management Access Options

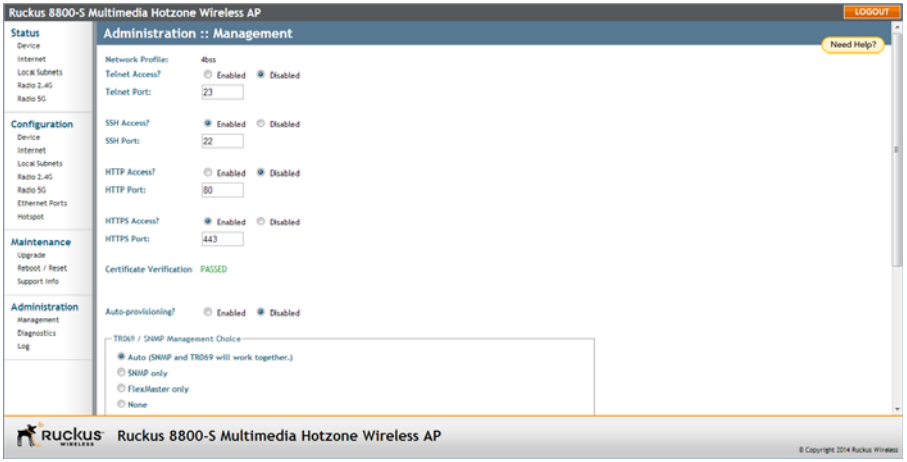
In addition to managing the AP via a Web browser using HTTPS, several other management access options are available on the AP. These options include management access using HTTP, Telnet and SSH.

You can also view and set up the connection to a Ruckus Wireless FlexMaster server under the **TR-069/SNMP Management Choice** options. If your ZoneFlex device is to be managed by FlexMaster, then the FlexMaster information (server URL and contact interval) is preconfigured before you receive your ZoneFlex device.

NOTE If you are configuring the AP to be managed by FlexMaster, then remember to point it to the FlexMaster server after you configure the management access options. For more information, refer to "Viewing FlexMaster Management Status" on page 124.

1 Go to **Administration** > **Management**.

Figure 53. The Administration > Management page



2 Review the access options listed in Table 37, and then make changes as needed.

Table 37. Management Access Options

Option	Description
Telnet Access	By default, this option is disabled (inactive).
Telnet Port	This field lists the default Telnet port of 23 — only if Telnet is active. You can manually change this port number, if required.
SSH Access	By default, this option is enabled (active).
SSH Port	This field lists the default SSH port of 22—only if SSH is active. You can manually change this port number if required.
HTTP Access	This option is disabled by default.
HTTP Port	This field lists the default HTTP port of 80, if HTTP has been activated. You can manually change this port number if required.
HTTPS Access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the device.
HTTPS Port	This field lists the default HTTPS port of 443—only if HTTPS has been activated. You can manually change this port number if required.
Certificate Verification	This notes whether the security certificate linked to the HTTPS settings has been verified (*PASSED*) or not.
Auto-provisioning	This setting is disabled by default, and should only be enabled if using a FlexMaster server for AP management.
Start Recovery SSID after ___ seconds of connectivity loss	When connectivity is lost for this time, the recovery process is invoked. Default is 300 seconds. Enter 0 to disable this function. Only available on selected APs.
Continue service WLANs when in recovery mode	When the recovery process is invoked, the WLAN service is continued (**Enabled**) or halted (**Disabled**). Only available on selected APs.

3 If you want to use TR-069 or SNMP to manage the AP, then configure the settings listed in Table 38.

Table 38. TR-069 and SNMP Management Options

Option	Description
Auto	Enables the ZoneFlex device to be managed by either SNMP server, Ruckus Wireless ZoneDirector, or Ruckus Wireless FlexMaster.
SNMP only	Only allow SNMP management.
FlexMaster only	Only allow FlexMaster management.
DHCP Discovery	URL of server providing DHCP.
FlexMaster Server URL	URL of the FlexMaster server.
Digest-Authentication Username/Digest-Authentication Password	This information is automatically generated by the AP and used for authentication with FlexMaster. Change this value *only* if you want the AP to connect to another access control server (ACS).
Periodic FlexMaster Inform Interval	Interval at which the device should attempt to contact FlexMaster.

4 Click **Update Settings** to save your changes. A confirmation message appears at the top of the page.

You have completed configuring the management access options.

NOTE Remember to open any relevant firewall ports between the AP and the firmware upgrade/management server. For example, if HTTPS is used for firmware upgrades, open TCP port 443 on the firewall to allow connections through port 443. If FlexMaster server is used, open TCP ports 80 and 443 for HTTP/HTTPS communications, and TCP port 8082 for AP wake-up commands.

Viewing FlexMaster Management Status

If you configure the AP to be managed by FlexMaster, you can view the *TR-069 Status* section by scrolling to the bottom of the **Administration** > **Management** page.

Figure 54. TR-069 status information

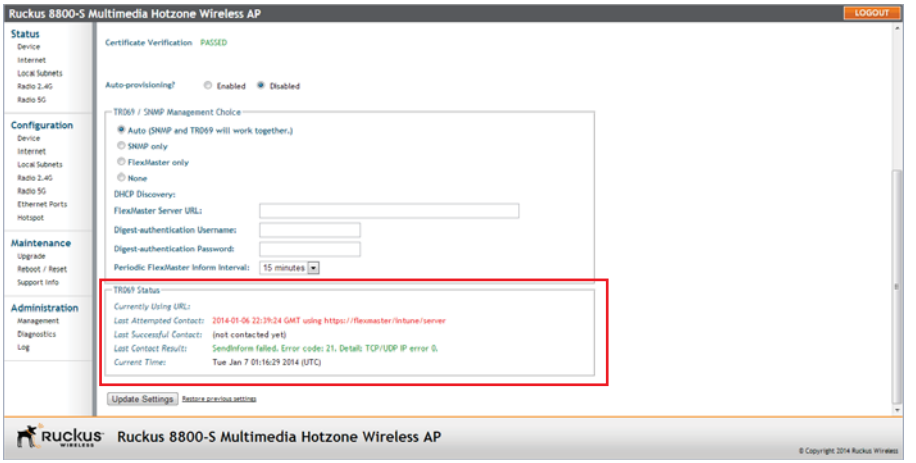


Table 39 lists the TR-069 status information that the AP provides.

Table 39. TR-069 status information

Status Information	Description
Currently using URL	Shows the FlexMaster server IP address or URL with which the AP is currently registered.
Last Attempted Contact	Shows the date and time of the AP's last attempt to contact FlexMaster. Date and time are specified in GMT (or UTC), which are accurate if a Network Time Protocol (NTP) server is configured.
Last Successful Contact	Shows the date and time of the AP's last successful contact with FlexMaster.
Last Contact Result	Shows the result of the last attempt to contact FlexMaster (success or failure, and failure error code if applicable).

Table 39. TR-069 status information (Continued)

Status Information	Description
Current Time	Shows the current date and time as known to the AP. This timestamp is accurate if an NTP server is configured on the AP. If there is no NTP server configured, this timestamp is useful as a reference for comparison of the timestamps for *Last attempted contact* and *Last successful contact.*

Pointing the AP to FlexMaster

Your ZoneFlex device is required to "call home" to register with your FlexMaster; FlexMaster does not initiate initial contact. To register successfully with FlexMaster, your ZoneFlex device must know the FlexMaster server's URL. You need TCP ports 80 and 443 open between APs and FlexMaster when traversing Layer 3/firewall boundaries.

1 Go to **Administration > Management**.

2 Under *TR-069/SNMP Management Choice,* click **Auto**.

3 In *FlexMaster Server URL,* type the URL of the FlexMaster server.

4 Toggle the *Periodic FlexMaster Inform Interval* drop-down list to select how frequently the device checks the FlexMaster server for any pending configuration changes available for that ZoneFlex unit. On the FlexMaster side, this field is referred to as the *Periodic Inform Interval.*

5 Click **Update Settings** to save your changes.

After the AP registers with FlexMaster, this **Administration > Management** page shows the communication status between the AP and FlexMaster.

Working with Event Logs and Syslog Servers

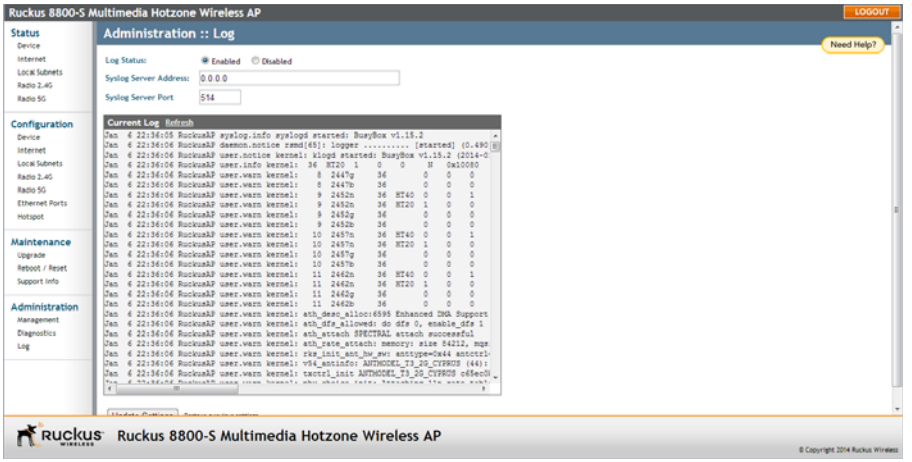
Both the *Maintenance* > *Support Info* and *Administration* > *Log* pages can be used to view the AP's current log file text. You can use the former to send the log to Ruckus Wireless support or save it to a local file, and use the latter to configure automatic delivery of log files to a syslog server.

Enabling Logging and Sending Event Logs to a Syslog Server

If you have a syslog server on the network, you can configure the Access Point to send the device logs to the server. Enable logging (if disabled) and configure the Access Point to send logs to the syslog server.

1 Go to **Administration** > **Log**. The *Administration* > *Log* page appears.

Figure 55. The Administration > Log page



2 In *Log Status,* click **Enabled**.

3 After enabling logging, configure the following options:

- *Syslog Server Address:* To enable the AP to send messages to a syslog server as they appear, enter the IP address of the syslog server.
- *Syslog Server Port:* By default, the syslog port number is 514. If the syslog server is using a different port, enter that port number in this field.

4 Click **Update Settings** to save and apply your changes.

Sending a Copy of the Log File to Ruckus Wireless Support

The Support Info log consists of the configuration and run-time status of the AP and can be useful for troubleshooting. You have three options for sending a copy of the current log file to Ruckus Wireless Support:

- Save a copy to your local PC, then attach it to an e-mail message and send it to support.
- Set up a connection to an FTP site.
- Set up a connection to a TFTP site.

1 Go to **Maintenance** > **Support Info**. The *Maintenance* > *Support Info* page appears.

2 To upload a copy of the support info file to an FTP or TFTP server, click the *Transfer Method* **TFTP** or **FTP** option.

3 In *Server Address,* enter the FTP or TFTP server IP address.

4 In *Filename,* enter a name for the file that you are saving.

NOTE Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host."

---

5 If you selected the **FTP** option, then also enter a *Username* and *Password.*

6 Click **Upload Now**.

Saving a Copy of the Log File to Your Computer

You can save a copy of the current log to your own computer, if needed.

1 Go to **Maintenance** > **Support Info**. The *Maintenance* > *Support Info* workspace appears.

2 Click the *Transfer Method* **Save to Local Computer** option. Up to three links appear next to **Download** (*supportinfo.txt*, *cmsupportinfo.txt* and/or *tr069info.txt*).

3 Click the **supportinfo.txt** link. A new window (or tab) opens with the content of the log file displayed.

4 Choose **Save As** or **Save Page As** from your browser's *File* menu.

5 When the "Save as..." dialog box appears, find a convenient location on your local computer to save the file, and change the file extension from *.html* to *.txt*.

6 Click **Save** to save the log file to your computer.

Saving a Copy of a Support File to Your Computer

You can save a copy of the support file(s) to your own computer, if needed. The *cmsupportinfo.txt* file includes support information for an AP with integral cable modem (such as 7781CM), and the *tr069info.txt* file includes support information for an AP being managed by FlexMaster.

1 Go to **Maintenance** > **Support Info**. The *Maintenance > Support Info* workspace appears.

2 Click the *Transfer Method* **Save to Local Computer** option. Up to three links appear next to **Download** (*supportinfo.txt*, *cmsupportinfo.txt* and/or *tr069info.txt*).

3 Click the **cmsupportinfo.txt** or **tr069info.txt** link. A new window (or tab) opens with the content of the support file displayed.

4 Choose **Save As** or **Save Page As** from your browser's *File* menu.

5 When the "Save as..." dialog box appears, find a convenient location on your local computer to save the file, and change the file extension from *.html* to *.txt*.

6 Click **Save** to save the support file to your computer.

Upgrading the Firmware

You can use the Web interface to check for software updates/upgrades for the firmware built into the AP. You can then apply these updates to the device in one of two ways: (1) manual updating on an as-needed basis or (2) automating a regularly scheduled update.

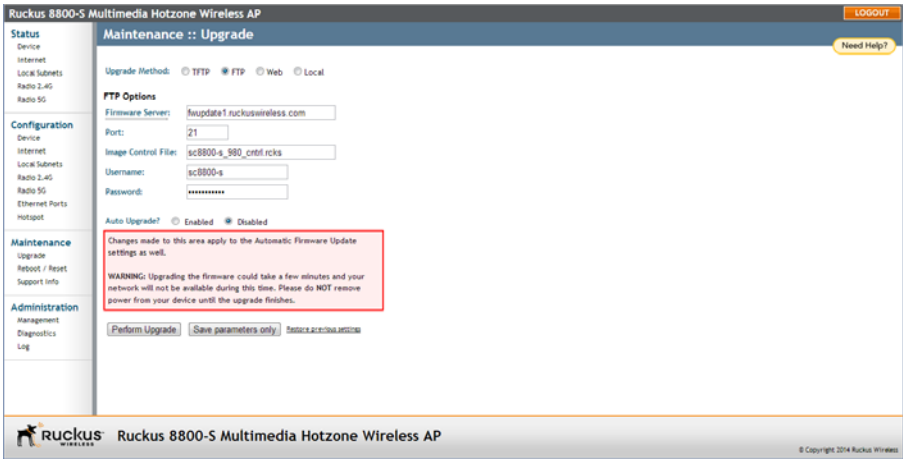
Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now

By default, the automatic upgrade option is disabled.

To get started with upgrading the firmware, go to **Maintenance** > **Upgrade**. When the *Maintenance* > *Upgrade* options appear, decide which upgrade method to use. Each of the upgrade options listed on the *Upgrade* page are discussed in the following sections.

Figure 56. The Maintenance > Upgrade page



Upgrading Manually via FTP or TFTP

1 In the *Upgrade Method* options, click **FTP** or **TFTP**.

2 Click the host name field, and then type the URL of the server. Or click the IP address field, and then type the IP address of the server. Remember to start the URL with **`ftp://`**.

CAUTION! Do not change any of the *Image Control File, Username* or *Password* entries.

3 Click **Perform Upgrade**. A status bar appears during the upgrade process.

4 After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via the Web

1 In the *Upgrade Method* options, click **Web**.

2 If instructed to choose a different URL than the default value, type the URL of the download Web site in **Url.** Remember to start the URL with **`http://`**.

3 Click **Perform Upgrade**. A status bar appears during the upgrade process.

4 After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via Local File

If you have already saved a firmware file on your local computer, you can upgrade directly using the Web interface.

1 In the *Upgrade Method*, select **Local**.

2 Click **Choose File** and locate the file on your local computer.

3 Select the file and click **Open**.

4 Click **Perform Upgrade**. A status bar appears during the upgrade process.

5 After the upgrade is completed, you must manually reboot the AP.

Scheduling Automatic Upgrades

1 In the *Upgrade Method* options, click the button for your preferred choice.

2 Enter the appropriate information in the *Host name* or *IP address* field.

CAUTION! Do not change any of the *Image Control File, Username* or *Password* entries.

3 Verify that the *Auto Upgrade* option is set to **Enabled**.

4 Toggle the *Interval to Check for Software Upgrade* drop-down list to select your preferred interval.

5 Choose whether to reboot immediately after upgrading, or schedule the reboot for a specific time of day using the *Schedule Reboot Time After Upgrade* list. Choosing **Any Time** (the default value) results in the AP performing a reboot immediately after the automatic upgrade is successful.

6 You have two options at this point:

- Click **Perform Upgrade**, which starts the process and the clock. The next upgrade occurs at the selected interval.
- Click **Save parameters only**. The clock starts right away, and the actual upgrade occurs at the first effective interval.

After you click one of these two options, a status bar appears during the upgrade process.

When the upgrade is complete, the AP automatically reboots at the time you specified in Step 5.

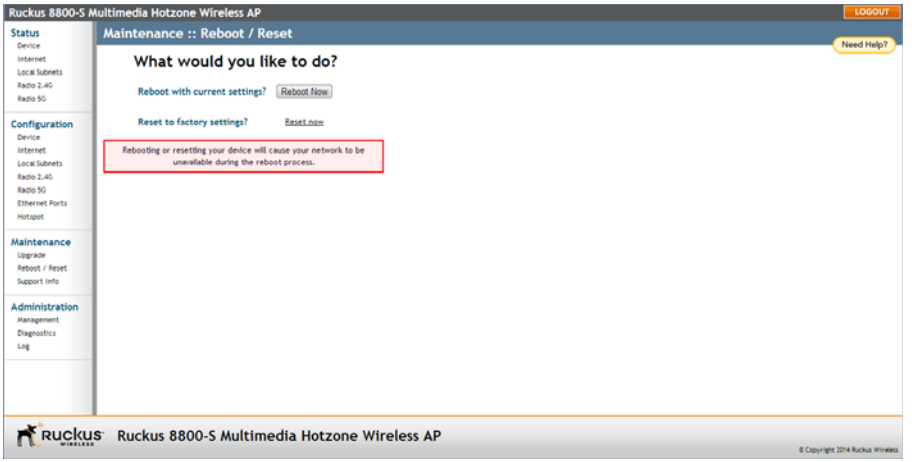
Rebooting the AP and Cable Modem

You can use the Web interface to prompt the AP to reboot, which restarts the AP without changing any of the current settings. If your AP is equipped with an integral Cable Modem (such as a 7781CM), then you can use the AP Web interface to prompt the CM to reboot, which restarts the CM without changing any of the current settings.

Please note that rebooting the AP or CM disrupts network communications in any currently active WLANs.

1. Go to **Maintenance** > **Reboot/Reset**. The *Maintenance* > *Reboot/Reset* page appears.
2. To reboot the AP, click *Reboot AP with current settings*/**Reboot Now**. After a brief pause, you are logged out of the AP.
3. To reboot the CM, click *Reboot Cable Modem*/**Reboot Now**. After a brief pause, you are logged out of the AP.

Figure 57. The Maintenance > Reboot/Reset page



After approximately one minute, you should be able to log back into the AP, which verifies that the reboot was successful. You can also check the LEDs on the AP to verify the status of the device.

NOTE The 7761-CM and 7781CM access points with integral cable modems can also be remotely reset using the OID and CLI commands described in the *ZoneFlex 7761-CM* and *7781CM Installation Guides*.

Resetting the AP to Factory Defaults

WARNING! DO NOT reset the Access Point to factory defaults unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately reconnect the restored AP to your computer, to reconfigure it for Wi-Fi network use — as detailed in "Logging Into the ZoneFlex AP Web Interface" on page 64.

You can use the Web User interface to restore an inoperative AP to its factory default settings, which completely erases the configuration currently active in the device. Note that this disrupts all wireless network communications through this device.

1. Go to **Maintenance** > **Reboot/Reset**. The *Maintenance* > *Reboot/Reset* page appears.
2. Click **Reset now** (next to *Reset the AP to factory settings*).
3. When the confirmation warning appears, read the message and click **OK** if you are certain that you want to restore the AP to factory defaults.

After a brief pause, you are automatically logged out of the AP. You must now disconnect the AP from the switch (and the network) and reconnect it to your computer, as described in the associated AP *Installation Guide.* At this time, you can restore the network settings, then replace it in your site for full network use.

Running Diagnostics

Two network connection diagnostic tools, ping and traceroute, have been built into the AP to help you check network connections from the Web interface.

1 Go to **Administration > Diagnostics**. The *Administration > Diagnostics* page appears. Two options are available:

- *Ping*
- *Traceroute*

2 Click the text field by the option you want to activate, and type the network address of a site you wish to connect to.

3 Click **Run test**.

The results appear in the text field below each option.

Figure 58. Pinging an IP address

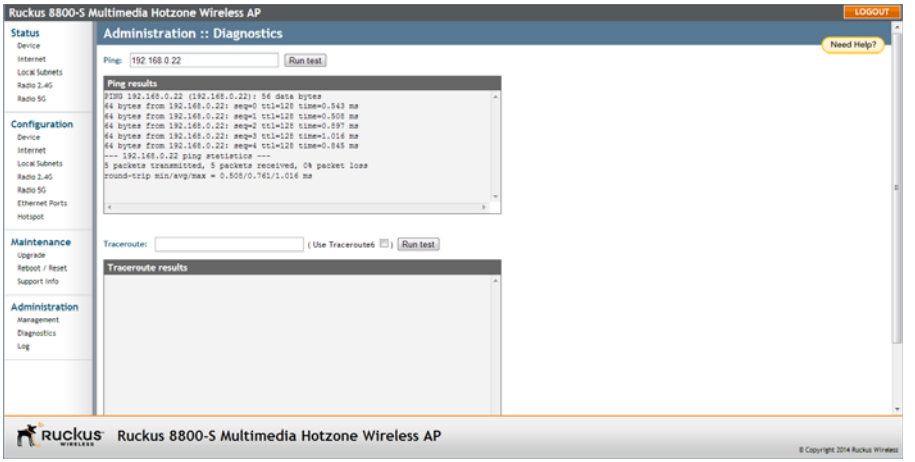
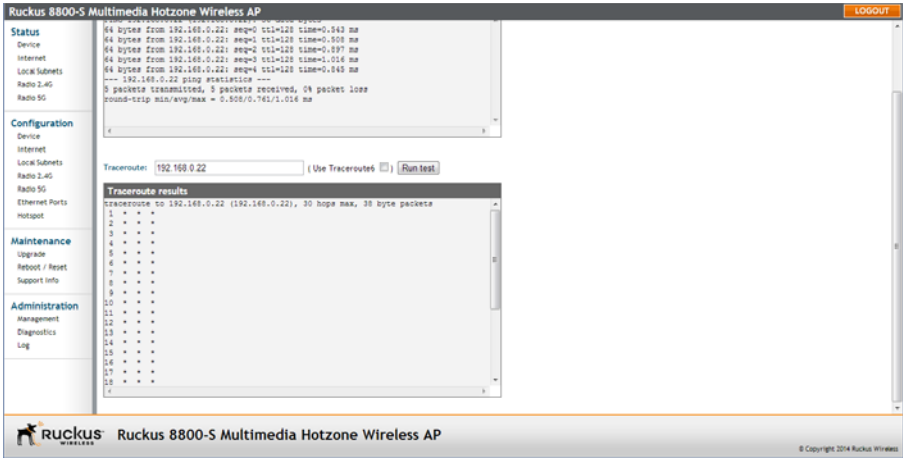


Figure 59. Running traceroute on ruckuswireless.com



Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at http://support.ruckuswireless.com. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.

Index

Numerics

7761-CM ZoneFlex AP 14
7762 ZoneFlex AP 19
7762-AC ZoneFlex AP 22
7762-S ZoneFlex AP 25
7762-S-AC ZoneFlex AP 28
7762-T ZoneFlex AP 31
7781CM ZoneFlex AP 34
7782 ZoneFlex AP 41
7782-E ZoneFlex AP 43
7782-N ZoneFlex AP 46
7782-S ZoneFlex AP 48
802.11ac AP
  T300 55
  T301n 58
  T301s 61
802.1Q 70
802.1X 101, 104
  configuration 93
  rate limiting 97
  WPA authentication 92
802.3af
  PoE out port 17, 20, 23, 26, 29, 32, 42, 47, 49

A

access control 97, 98
access control list options 97
access port 100
  definition 103
access VLAN 87
ACL options 97
administrative login 120
advanced settings, wireless 81
AeroScout 82
AES WPA algorithm 92, 94
algorithm
  WPA AES 92, 94
  WPA auto 92, 95
  WPA TKIP 92
AP factory defaults, resetting 133
AP, installing 12
associated clients 119
authenticated users login redirect URL 107
authentication
  WPA 802.1X 92
  WPA auto 92
  WPA PSK 92
auto WPA algorithm 92, 95
auto WPA authentication 92
auto WPA version 92, 94

B

basic settings, Hotspot 106
beacon interval 96
BeamFlex 11
beamforming, transmit 11
Bridge to L2TP Tunnel 87, 101
Bridge to WAN 87, 101
bridging, local 101
broadcast SSID 86

C

changing the login settings 68
channel
  width 81
  wireless 81
client fingerprinting 88
configuring WLANs 85
connection type
  DHCP (auto) 72
  IP static IP 74
  IPv4 PPPoE 75
country code 118
  wireless 81
CTS-only protection mode 85

D

data beacon rate 96
default IP address 71
default user name and password 64
delivery traffic indication message 96
device
  location 68

name 68
settings 68
DHCP
release 72, 73, 74
renew 72, 73, 74
DHCP (auto) connection type 72
DHCP Option 82 88, 102
diagnostics 134
DTIM 96
dynamic VLAN 87

E

Ekahau 82
enable/disable individual ethernet port 100
encryption 88
ethernet individual port types 100
ethernet port
configuration 100
enable/disable 100
ethernet port types 100, 103
external antenna 82
external antenna gain 82

F

factory defaults, resetting AP 133
firmware upgrade 129
FlexMaster 11
FlexMaster management status 124
FlexMaster server URL 123
forwarding, packet 101

G

general port 100
definition 104
GPS coordinates 68
guest VLAN 102

H

heater, internal 68
help 65
Hotspot
basic settings 106
network settings 106
optional settings 107
unrestricted access 111
walled garden 110

I

installing an AP 12
internal heater 68
Internet settings 70
interval, beacon 96
IP address 71
IPv4 connection type 72
IPv6 connection type 72
Isolated 87, 101

K

key index, WEP 90

L

L2TP 76
LED control 68
local bridging 101
local subnet 78, 87, 101
Local Subnet NAT and Route to WAN 87, 101
logging in 64
login redirect URL
authenticated users 107
unauthorized users 106
login remote authentication 69
login settings 68
logout 65

M

MAC authentication bypass 105
management access options 121
menu 65
mode
standalone 11
wireless 81

N

name, device 68
network 86
network settings, Hotspot 106
network time protocol server 71

O

optional settings, Hotspot 107

P

packet forwarding 87, 101
passphrase, WPA 92
ping 134
PoE out port 68
  802.3af 17, 20, 23, 26, 29, 32, 42, 47, 49
port
  access 100
  general 100
  trunk 100
port type
  ethernet 100
port-based VLAN 100, 104
PPPoE IPv4 connection type 75
protection mode
  CTS-only 85
  RTS/CTS 85
PSK WPA authentication 92

R

radio network, wireless common 81
rebooting 132
releasing DHCP 72, 73, 74
renewing DHCP 72, 73, 74
resetting an AP to factory default 133
RFID
  AeroScout 82
  Ekahau 82
router mode 78
RTS/CTS
  protection mode 85
  threshold 96

S

SC8800-S 50
service provider login 69
SSID 86
standalone mode 11
static IP connection type 74
syslog 126

T

T300 AP 55
T301n AP 58
T301s AP 61
tabs 65
TACACS+ server 69
tags
  AeroScout 82
  Ekahau 82
temperature update 68
threshold 86
  RTS/CTS 96
TKIP WPA algorithm 92
traceroute 134
transmit beamforming, TxBF 11
transmit power 84
trunk port 100
  definition 103
Tunnel via L2TP 87, 101
TxBF transmit beamforming 11

U

unauthorized users login redirect URL 106
unrestricted access, Hotspot 111
URL
  authenticated users login redirect 107
  FlexMaster server 123
  unauthorized users login redirect 106
user name 69

V

version, WPA
  auto 92, 94
  WPA 92
  WPA2 92, 94
viewing associated clients 119
VLAN 100, 102
  dynamic 87
  guest 102
  overview 70
  wired 104
  wireless 87

W

walled garden, Hotspot 110
web interface 64
WEP 88
WEP key index 90
width, channel 81
wireless 86
  advanced settings 81
  channel 81

country code 81
mode 81
wireless availability 86
wireless channel 118
wireless common
radio network 81
wireless mode 117
wireless network 86
wireless security
802.11X 93
WEP 88
WPA 90
wireless settings 80
WLAN configuring 85
workspace 65
WPA 90
802.1X authentication 92
auto authentication 92
passphrase 92
PSK authentication 92
WPA version
auto 92, 94
WPA 92
WPA2 92, 94
WPA2 WPA version 92, 94

Z

ZoneDirector 11
ZoneFlex
7761-CM AP 14
7762 AP 19
7762-AC AP 22
7762-S AP 25
7762-S-AC AP 28
7762-T AP 31
7781CM AP 34
7782 AP 41
7782-E AP 43
7782-N AP 46
7782-S AP 48
ZoneFlex smart WLAN system 11

Copyright © 2006-2014. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com